KEAMANAN WEB SERVER DENGAN SISTEM LINUX DEBIAN (Studi Kasus Universitas Islam Kebangsaan Indonesia)

Chaeroen Niesa
FKOM Universitas Islam Kebangsan Indonesia
jeumalaniesa@gmail.co

ABSTRAK

Sistem keamanan dalam mengakses jaringan komputer merupakan sebuah hal yang sudah sangat perlu di perhatikan karena sudah banyaknya media komunikasi menggunakan web untuk menyampaikan informasi. Dalam hal keamanan web, para pengguna media internet paling sering terkena serangan yang berupa penyadapan data, hal ini akan sangat merugikan para penggunajika data mereka yang penting di curi orang. Salah satu teknik untuk mengatasi penyadapan dapat dilakukan dengan teknik enkripsi jaringan data menggunakan HTTPS. Sehingga setiap data yang di akses oleh pengguna tidak dapat di baca oleh pihaklain. Pengamanan dengan teknik ini akan penulis uji coba dan akan menjelaskan hasilsebagai acuan pada admin jaringan dalam mengamankan website.
Kata Kunci: Website, Keamanan, HTTPS.

PENDAHULUAN

Kebutuhan system informasi saat ini sangat berkembang pesat, baik dari segi pendidikan, penjualan, bisnis, bahkan pemerintahan. Sistem informasi yang banyak digunakan saat ini adalah yang berbasis web site, di mana informasi yang diberikan dapat lebih mudah diakses dan memiliki segala fitur yang dibutuhkan untuk penyebaran informasi.

Banyaknya jasa hosting gratis yang tersedia saat ini, banyak instansi tertentu membangun sendiri sistem websitenya sehingga dapat dikelola dengan lebih leluasa dan sistem yang lebih komplit. Dengan banyaknya website yang tersedia baik yang komersial atau bisnis semua itu sudah memerlukan sebuah keamanan untuk mengaksesnya sehingga para pengguna dapat lebih aman dalam melakukan banyak transaksi pada website tersebut.

Salah satu hal yang sering terjadi dalam pengaksesan website adalah proses penyadapan transmisi data yang sedang berlangsung. Banyak penyadapan website bertujuan untuk mendapatkan akses ke website dengan memperoleh username dan password, tentun yaitu menjadi sebuah kerentanan dalam pengaksesan website sehingga sistem keamanan pada website sangat diperlukan untuk website yang mengandung banyak transaksi penting di dalamnya.

Cara mengatasi hal tersebut adalah dengan memasang sebuah system keamanan website yang di sebut Secure Socket Layer (SSL), website yang sudah dipasangkan SSL akan sedikit berbeda pada saat pengaksesanya itu terdapat HTTPS:// pada link website tersebut. Sistem kerja darai SSL ini adalah pada saat transmisi data berlangsung antara user dan website, data yang dilewatkan akan di enkripsi terlebih dahulu sehingga ketika ada penyadapan terhadap transaksi tertentu, data tersebut tidak dapat dibaca oleh penyadap dan akan susah untuk diterjemahkan dalam bahasa sehari-hari.

Sistem keamanan website dengan SSL iniakan di pasangkan pada server linux debian dengan contoh pengaksesan website berbasis client server. Sistem yang berbasis linux akan lebih stabil dan dapat terhindar dari serangan cracker karena dapat di kelolase demikian rupa sehingga sistemnya dapat menjadi lebih aman dan terhindar dari virus.

METODE PENELITIAN

GambaranUmumSistem

Sistem keamanan website adalah salah satu sistem yang cukup dibutuhkan untuk sekarang ini, karena sudah banyak website yang sudah menggunakan transaksi langsung pada web tersebut

seperti Bank dan Penjualan Barang Online. Begitu juga website yang mempunyai banyak data penting seperti website sekolah atau sebuah kampus, yang perlu pengamanan yang cukup bagus ketika user mengakses data tersebut sehingga tidak terjadi penyadapan data oleh orang yang ingin mengambil data tersebut secara illegal.

Analisa SistemSebelumnya

Pada system sebelumnya setiap komputer yang terhubung dan menggunakan fasiliatas internet untuk mengakses webserver merupakan hal yang tidak aman bagi website yang memiliki otoritas data yang penting bagi penggunanya.

Pada saat sekarang ini sudah banyak website yang telah dibajak oleh pengguna yang tidak bertanggungjawab, terutama proses transaksi yang menggunakan media website. Hal ini tentu saja membuat pengguna khawatirakan terjadi ketika mereka mengakses situs tertentu, penyadapan akan dilakukan pada saat pengguna melakukan login dan lain sebagainya sehingga penyadapakan mendapatkan informasi penting seperti username dan password pengguna.

Gambar 1. Sistem penyadapan Website

Solusi untuk mengatasi penyadapan tersebut adalah dengan mengamankan website atau web server utamanya menggunakan system enkripsi website atau sering disebut SSL atau HTTPS. SSL dapat mengamankan proses trasmisi data dari webserver terhadap client. Penggunaan SSL biasanya diterapkan pada website yang memerlukan pengamanan data seperti data bank, kartu kredit, dan informasi pribadi penting lainnya. Website bisnis biasanya dilengkapi dengan sertifikat SSL pada websitenya untuk menjaga kerahasiaan data para klien atau membernya. Dengan memasang SSL, semua transaksi dan pertukaran data yang terjadi antara remote komputer dan server akan sepenuhnya aman. Selain itu memasang SSL bias meningkatkan kepercayaan member / klien terhadap kinerja website.

Spesifikasi Kebutuhan Sistem

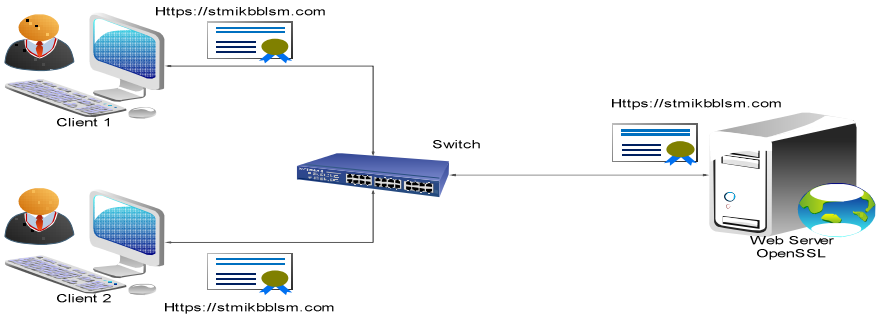
Dalam penelitian ini kebutuhan system terbagi dua macam, yaitu kebutuhan *hardware* dan *software*, di mana keduanya saling mendukung satu sama lain.

a. Kebutuhan Hardware
1. Swicth/Hub 8 Pin
2. Kabel UTPCategori 5E
3. KomputerServer

b. Kebutuhan Software
1. Linux Debian Wheezy
2. Apache2, PHP5, BIND9
3. Paket OpenSSL
4. Wireshark

PerancanganSistem

Sebelum membangun sebuah sistem keamanan webserver terlebih dahulu menentukan perancangan dari sistem tersebut. Sehingga akan memudahkan penulis untuk membangun sistem tersebut.

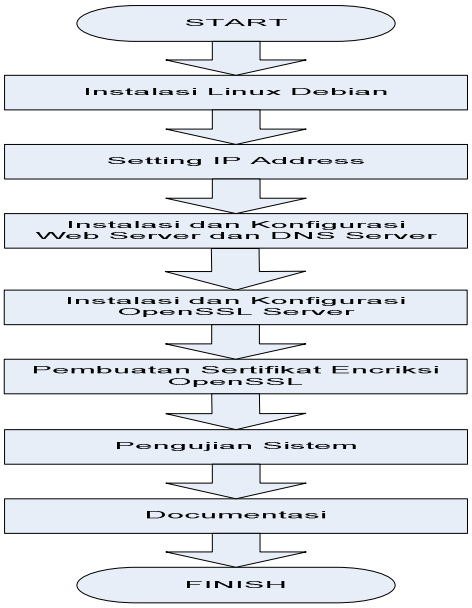


Gambar 2. Perancangan Jaringan Web server

Perancangan pada gambar 2, menunjukkan alur hubungan antar sistem *server* dan client dalam mengakses web server yang dihubungkan oleh sebuah switch. Dengan perancangan tersebut penulis akan membangun sebuah sistem yang dapat mengamankan jalur komunikasi data antara client dan server sehingga penyerang/penyadap tidak bisa memantau data yang sedang diproses oleh client.

Alur Perancangan Sistem

Alur dan perancangan sistem digunakan untuk menggambarkan rancangan dan tahapan-tahapan sistem keamanan web server. Adapun tahapan yang diperlukan dapat dijabarkan dalam bentuk *flowchart* seperti yang ditunjukan pada gambar 3. di bawah ini.



Gambar 3. Perancangan Sistem

HASIL DAN PEMBAHASAN

Implementasi Sistem

Pada tahap ini dilakukan implementasi terhadap sistem yang telah dibuat apakah berjalan sesuai dengan perancangan, maka akan dilakukan pengujian pada sistem yang telah dirancang. Pengujian ini menggunakan sebuah computer server dan dua buah client yang di

antaranya client 1 menggunakan sistem operasi windows dan client 1 sebagai penyadap menggunakan aplikasi wireshark.

Konfigurasi Server

Konfigurasi dilakukan pada sistem server untuk mensetting beberapa hal seperti setting IP Address, setting DHCP, setting DNS Server, setting Web Server dan setting s stem keamanan pada Web Server.

Konfigurasi IP Address

Sebelum melakukan konfigurasi IP Address, ketikkan perintah sudosu pada terminal, kemudian masukkan password root.

Untukkonfigurasi IP address gunakan perintah :

nano /etc/network/interfaces

Lalu tambahkan script seperti gambar 4.

Gambar 4. Setting IP Address

Interface eth0 digunakan untukjaringan public yang terhubung ke internet dan interface eth1 digunakan untuk jaringan private yang terhubung ke client local. Setelah selesai konfigurasi, kemudian restart service network dengan menggunakan perintah berikut :

/etc/init.d/networking restart

Lalucek IP yang telah dikonfigurasi dengan menggunakan perintah

ifconfig

Gambar 5. Hasil Ifconfig

PENUTUP

Simpulan

1. Penerapan sistem keamanan Web Server pada sebuah komputer server berhasil di lakukan dengan mengkonfigurasi beberapa file yang ada pada paket web server dan melakukan konfigurasi keamanannya pada openssl.

2. Client yang terhubung dengan server mendapat ip address secara otomatis karena sudah di setting dhcp server sehingga client bias langsung berhubungan dengan satu sama lain tampa harus mengesetip address secara manual pada setiap komputer client.
3. Website yang sudah diamankan oleh Https akan melakukan enkripsi data secara otomatis kapanpun client mengakses web tersebut.
4. Sistem keamanan web server dapat diakses pada setiap client dengan link https://stmikbb-lhokseumawe.com dengan hasil yang telah diuji dapat dijalankan pada platform manapun dan browser yang mendukung google crome, firefox, opera.

Saran

1. Sistem ini dapat menggunakan database server untuk web server nya sehingga penggunaan web server akan lebih baik dan dapat mengelola data.
2. Menambahkan fitur kemanan yang lainnya yang dapat mendukung keamanan di server.

DAFTAR PUSTAKA

Achmad, Solichin. 2009. Pengenalan *Web Server* dan *Server Side Scripting.* Russel George. Fakultas Teknologi Informasi. Jakarta.

Bambang, Wilfridus. 2008. *Pengenalan Linux & Debian*. UK Maranatha. Bandung.

Kimin. 2011. *Pencegahan Penyusupan Dengan Menggunakan Snort*. Universitas Sumatera Utara.

Rushadi, Syukron. 2012. *Konsep Keamanan Jaringan Komputer Dengan Infrastruktur Demilitarized_Zone*. Universitas Sriwijaya. Palembang.