BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi dan komunikasi (TIK) telah menjadi bagian hidup manusia yang tidak dapat dipisahkan. Keberadaan TIK membuat hidup kita menjadi lebih mudah dan menyenangkan. Aktivitas yang terkait dengan pekerjaan, pendidikan, hingga hiburan terkait erat dengan pemanfaatan TIK. Menyusun dokumen elektronik, melakukan penghitungan, mengirim dan membaca *e-mail*, berselancar di *internet*, *chatting* merupakan aktivitas sehari-hari yang memanfaatkan TIK. Tidak ada satupun organisasi atau perusahaan yang tidak menggunakan peralatan TIK dalam kegiatannya, bahkan bagi sebagian mereka, TIK sudah menjadi bagian utama pelaksanaan kegiatan.

Layaknya dunia nyata, dalam dunia TIK selain hal-hal baik yang diperoleh, ada juga hal-hal buruk yang mengintai, antara lain seperti penyebaran virus komputer dan *spam*, aktivitas *cracking* dan *sniffing*, dan sebagainya. Kita harus menerima kenyataan bahwa ada orang yang bermaksud tidak baik diluar sana.

Kejahatan dalam bidang teknologi informasi dengan melakukan serangan elektronik berpotensi menimbulkan kerugian pada bidang politik, ekonomi, sosial budaya, yang lebih besar dampaknya dibandingkan dengan kejahatan yang

berintensitas tinggi lainnya. Di masa datang, serangan elektronik dapat mengganggu perekonomian nasional melalui jaringan yang berbasis teknologi informasi seperti perbankan, telekomunikasi satelit, listrik dan lalu lintas penerbangan. Hal ini dipicu oleh beberapa permasalahan yang ada dalam konvergensi teknologi, misalnya *internet* membawa dampak negatif dalam bentuk munculnya jenis kejahatan baru, seperti *hacker* yang membobol komputer milik *bank* dan memindahkan dana serta merubah data secara melawan hukum. Teroris menggunakan *internet* untuk merancang dan melaksanakan serangan, penipu menggunakan kartu kredit milik orang lain untuk berbelanja melalui *internet*. Perkembangan TI di era globalisasi akan diwarnai oleh manfaat dari adanya *e-commerce, e-government, foreign direct investment*, industri penyedia informasi dan pengembangan UKM.

Web services merupakan sebuah kemajuan teknologi terbaru di bidang IT. Teknologi ini menjadi sedemikian populer karena kemampuannya mengintegrasikan aplikasi-aplikasi *web* yang berbeda *platform* satu sama lain. *Web services* mampu melakukan hal tersebut dengan keberadaan XML (*eXtensible Markup Language*), protokol SOAP (*Simple Object Access Protocol*) dan bahasa WSDL (*Web Services Definition Language*) serta UDDI (*Universal Discovery Description Language*).

Kemampuan *web services* itu tentunya sangat dibutuhkan, terutama dalam dunia *enterprise*. Dimana keterhubungan antara dua bisnis proses (yang dikelola dalam suatu aplikasi *web*), baik dalam skala intra organisasi maupun inter organisasi,

sangat dibutuhkan. Namun, upaya integrasi itu selama ini sering terkendala oleh perbedaan *platform* antara masing-masing aplikasi sehingga tidak memungkinkan adanya pertukaran data. Oleh karena itu, banyak *enterprise* yang sudah mulai melirik *web services* untuk diimplementasikan dalam proses bisnis mereka.

Namun dibalik kelebihannya itu, *web services* masih menyimpan beberapa kekurangan yang cukup krusial. Kekurangan-kekurangan inilah yang masih menahan banyak *enterprise* untuk tidak segera mengimplementasikan *web services* dalam bisnis mereka. Salah satu kendala yang paling dominan disini adalah masalah keamanan

Web services masih menyimpan banyak kerentanan pada model sistemnya. Teknologi keamanan yang ada sekarang ini dirasa belum cukup untuk mengatasi isu keamanan dalam *web services*. Mayoritas teknologi keamanan jaringan yang ada saat ini hanya bekerja pada *transport layer*. Sementara *web services* membutuhkan lebih dari itu. *Web services* membutuhkan pengamanan sampai pada *level application layer*. Pengamanan bukan hanya dilakukan terhadap setiap *bit* data yang ditransfer melalui jaringan tapi juga pengamanan pemrosesan data oleh aplikasi *web*nya.

Modsecurity adalah sebuah modul keamanan aplikasi web yang dapat bekerja dengan baik sebagai *reverse proxy* yang berfungsi untuk melindungi dari berbagai macam serangan aplikasi web dan memungkinkan untuk memonitor lalu lintas HTTP. Perangkat lunak ini merupakan proyek open source yang bertujuan untuk

membuat aplikasi web teknologi firewall yang tersedia untuk semua pengguna komputer[1].

Masalah keamanan merupakan salah satu aspek penting dari sebuah *web server apache*, namun sayangnya masalah keamanan *web server apache* ini kurang mendapat perhatian dari manajemen PT. Menara Terus Makmur. Bisa dibayangkan jika para penyusup (*attacker*) bisa mengambil alih *web server apache* dari jarak jauh maka para penyusup (*attacker*) tersebut tidak perduli apakah informasi di dalam *web server apache* tersebut iformasinya tidak terlalu penting (maksudnya disini adalah tampilan *website* hanya deskripsi, profil, visi dan misi, serta produk-produk baru PT. Menara Terus Makmur) tetapi target para penyusup (*attacker*) profesional disini adalah kemungkinan untuk dapat masuk ke dalam *Local Area Network* (LAN) PT. Menara Terus Makmur melalui perantara *web server apache* dan mencari informasi penting seperti *file* yang berhubungan dengan laporan keuangan, strategi perusahaan, dan *database client*, yang seharusnya informasi tersebut hanya dikonsumsi untuk kalangan manajemen PT. Menara Terus Makmur, ternyata berhasil disadap oleh para penyusup (*attacker*), dan tidak menutup kemungkinan jika ternyata para penyusup (*attacker*) tersebut tidak lain adalah pesaing bisnis dari PT. Menara Terus Makmur yang berusaha untuk menjatuhkan bisnis perusahaan tersebut.

[1] http://www.modsecurity.org, 22 Mei 2010

PT Menara Terus Makmur sebagai salah satu bagian dari ASTRA *Otoparts*, merupakan perusahaan yang bergerak dalam industri *forging*, *mechanical jack*, dan *dies shop*. PT. Menara Terus Makmur memiliki *web server apache* dengan konfigurasi standar dan tidak di lindungi oleh aplikasi *firewall* di *level application layer*, setiap harinya *web server apache* tersebut terkoneksi ke *internet* selama 24 jam dan ini memungkinkan para penyusup (*attacker*) untuk melakukan peneterasi *remote file inclusion* dan *remote code execution* dari kelemahan celah keamanan pada *web server apache* tersebut, walaupun sudah ada *endian firewall* namun aplikasi tersebut hanya bekerja pada *level network layer* dan tidak mampu mendeteksi para penyusup di *application layer*.

Skripsi ini akan menjelaskan tentang proses instalasi dan konfigurasi *linux debian* 5.0.4, *apache server*, dan *mod security*, dan melakukan pengujian sistem keamanan aplikasi *web server apache* yang sudah dilengkapi dengan *firewall application* dengan beberapa motede penyerangan seperti *remote file inclusion* dan *remote code execution*. Dari penjelasan latar belakang diatas maka penulis memberikan judul pada skripsi ini dengan judul :

"PERANCANGAN SISTEM KEAMANAN *WEB SERVER APACHE* MENGGUNAKAN *MODSECURITY* DI PT. MENARA TERUS MAKMUR"

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka dapat dirumuskan masalah sebagai berikut :

1. Bagaimana membangun dan mengimplementasikan sistem keamanan pada *web server apache* menggunakan *modsecurity* di tingkat *application layer* ?
2. Bagaimana meminimalkan kelemahan celah keamanan pada *web server apache* ?

1.3 Batasan Masalah

Ruang lingkup dari skripsi ini dibatasi khusus untuk Membangun dan mengimplementasikan sistem keamanan pada *web server apache* menggunakan *modsecurity* di tingkat *application layer*.

1.4 Maksud dan Tujuan

a. Maksud

Berdasarkan latar belakang yang telah di uraikan, maksud dari penulisan skripsi ini adalah merancang sistem keamanan aplikasi web dari berbagai serangan penyusup atau *cyber crime* dengan menggunakan *mod security* pada *web server apache* di PT. Menara Terus Makmur. Adapun maksud lain dari penyusunan skripsi ini adalah sebagai salah satu syarat dalam pencapaian gelar strata satu (S1) pada Fakultas Teknik Universitas Bhayangkara Jakarta Raya.

b. Tujuan

Menindak lanjuti maksud di atas, maka tujuan dari penulisan skripsi ini adalah meminimalisir resiko celah keamanan yang timbul pada *web server apache* di PT. Menara Terus Makmur.

1.5 Metode Penelitian

Pada langkah penelitian ini penulis melakukan beberapa proses percobaan dalam prarancangan sistem keamanan *web server apache* dengan menggunakan modsecurity di PT. Menara Terus Makmur, langkah-langkah tersebut meliputi beberapa proses seperti melakukan peninjauan tentang penelitian-penelitian yang berkaitan dengan perancangan sistem keamanan *web server apache* dengan menggunakan *modsecurity* di PT. Menara Terus Makmur, tabel berikut ini menggambarkan tentang langkah demi langkah dan lamanya waktu yang dibutuhkan untuk melakukan penelitian perancangan sistem keamanan *web server apache* dengan menggunakan *modsecurity* di PT. Menara Terus Makmur yang merupakan rencana kegiatan penulis untuk menyelesaikan skripsi.

Tabel 1.1 Rencana Kegiatan

Keterangan	juni				Juli			
	I	II	III	IV	I	II	III	IV
Pemilihan tema, topik dan judul								
Identifikasi masalah								
Studi pustaka								
Perancangan dan konfigurasi								
Uji coba								
Implementasi sistem								
Kesimpulan								

Metode penelitian yang dilakukan penulis selama proses pembuatan skripsi adalah sebagai berikut :

1. Metode Kepustakaan

   Dilakukan dengan mempelajari buku-buku atau pustaka yang berhubungan dengan pokok pembahasan.

2. Metode Observasi

   Teknik ini dilakukan untuk memperoleh data dengan melakukan pengamatan langsung ke PT. Menara Terus Makmur sebagai pendukung

utama dalam menganalisa, membangun, dan mengimplementasikan sistem keamanan *web server apache* menggunakan *modsecurity* di tingkat *application layer*.

3. Metode Eksperimen

Salah satu teknik untuk melakukan pengumpulan data dengan melakukan eksperimen pada suatu objek penelitian yang akan menjadi target percobaan. Contohnya adalah penulis melakukan eksperimen pada *web server apache* yang tidak dilengkapi dengan *firewall application* di PT. Menara Terus Makmur dengan melakukan penyerangan seperti *Remote file inclusion* dan *remote code execution*. Jika ternyata penulis berhasil menembus *web server apache* tersebut selanjutnya penulis akan mencatat beberapa kelemahan yang terdapat pada *web server apache* yang tidak dilengkapi dengan *firewall application* tersebut dan dicarikan solusinya, seluruh kegiatan eksperimen ini akan dibahas pada bab 3. Proses perancangan dari solusi permasahalan pada bab 3 akan dibahas pada bab 4.

1.6 Sistematika Penulisan

Berikut ini merupakan sistematika penulisan yang digunakan oleh penulis antara lain :

BAB I : PENDAHULUAN

Merupakan permasalahan pokok yang diteliti yang berisi latar belakang masalah, identifikasi masalah, batasan masalah, rumusan masalah, tujuan dan manfaat penulisan, metodologi penelitian, sistematika penulisan.

BAB II : LANDASAN TEORI

Membahas teori yang diperlukan untuk menganalisa, membangun, dan mengimplementasikan sistem keamanan *web server apache* menggunakan *modsecurity* di tingkat *application layer* di PT. Menara Terus Makmur.

BAB III : ANALISA SISTEM YANG SEDANG BERJALAN

Pada bab ini dijelaskan mengenai gambaran umum PT. Menara Terus Makmur, analisa permasalahan, identifikasi permasalahan yang dihadapi dan usulan pemecahan masalah.

BAB IV : PERANCANGAN MODSECURITY PADA WEB SERVER APACHE

Dalam bab ini akan membahas mengenai perancangan *modsecurity* pada *web server apache* yang diusulkan dan merupakan solusi dari permasalahan yang dihadapi. Mulai dari instalasi ditribusi linux debian 5.0.4, paket-paket yang dibutuhkan untuk merancang serta membangun *web server apache* dan *modsecurity,* hingga proses konfigurasi dan melakukan uji coba hasil sistem keamanan *web server apache* menggunakan *modsecurity* dengan beberapa metode penyerangan seperti *remote file inclusion* dan *remote code execution*, dan masih adakah kemungkinan penyusup untuk mengakses *Local Area Network* (LAN) dari jarak jauh.

BAB V : PENUTUP

Pada bab terakhir ini akan dikemukakan kesimpulan hasil pembahasan bab sebelumnya dan saran-saran.

Lampiran

Lampiran ini berisi tentang biodata dan daftar riwayat hidup penulis serta skrip program *exploit* dan *modsecurity* yang merupakan bagian dari perancangan sistem keamanan *web server apache* dengan menggunakan *modsecurity* di PT. Menara Terus Makmur.