BAB I

PENDAHULUAN

1.1 Latar Belakang

Seperti halnya setiap teknologi baru selalu ada suatu hal positif dan aspek negatif, hal positifnya adalah ada peluang bisnis yang luar biasa dan sisi negatifnya adalah resiko keamanan yang sangat besar yang kini harus dihadapi oleh banyak perusahaan, namun hanya sedikit perusahaan yang sadar akan bahaya potensial, contoh resiko yang terjadi melalui jaringan *internet*, sejak perusahaan sudah menginvestasikan berjuta-juta uang di dalam infrastruktur ini, banyak hal yang mereka tidak sadari bahwa keamanan tidak hanya dilakukan di dalam tetapi di luar juga, dari hal tersebut banyak perusahaan terancam bahaya dan bersifat lemah, dengan *internet* mereka memperkenalkan profil perusahaannya dengan data-data yang mereka anggap penting untuk diketahui oleh orang banyak melalui media *website*, tetapi tidak sedikit orang yang memanfaatkan data-data tersebut untuk dimanipulasi dan dijadikan sebagai bahan untuk tindak kejahatan dengan cara menyebarkan informasi fiktif. Contoh kasus nyata yang terjadi di Indonesia adalah pada saat pemilihan umum

tahun 2004, dimana semua perolehan data dilaporkan secara *online* ke dalam komputer *sever* Komisi Pemilihan Umum (KPU) dan kemudian ditembus pertahanan komputernya oleh seorang peretas *(hacker)* dengan tujuan memanipulasi perolehan suara salah satu partai[1].

Metode yang digunakan oleh peretas dalam kasus pembobolan *server* KPU ini adalah metode yang biasa dikenal dengan istilah *cross site scripting (XSS)*[2], dimana metode ini mengandalkan kelemahan dari komputer korban atau biasa disebut dengan nama *vulnerability* yang dapat diidentifikasi melalui situs, setelah kelemahan itu ditemukan maka seorang peretas akan berusaha menyisipkan skrip baru kedalam situs korban, sehingga skrip asli dari *website* tersebut dapat dibaca oleh pengguna lain yang statusnya bukan administrator dari situs tersebut.

Kasus lain yang penulis kutip dari media pemberitaan Federal Bureau of Infestivigation (FBI), memberitakan tentang penangkapan seseorang pria yang berumur 24 tahun pada tanggal 23 Juli 2003 di New Scotland Yard, pria tersebut membuat dan memanipulasi kode berbahaya yang biasa dikenal dengan nama W32-leave.worm ke

[1] http://www.detikinet.com/read/2009/04/14/084702/1115008/398/pengejaran-hacker, 14 April 2009

[2] S'to, Seni Teknik Hacking I, Jasakom, Jakarta, 2004

dalam sistem komputer yang berbasis sistem operasi Microsoft Windows, kode berbahaya tersebut mampu memberikan izin kepada seorang penyusup untuk mengakses sebuah sistem komputer yang telah terinfeksi kode tersebut selama komputer korban terhubung dengan internet.[3]

Kasus yang terjadi di Indonesia hanyalah sebagian kecil dari kasus-kasus keamanan komputer yang ada di dunia, hal ini menyebabkan berkembangnya perusahaan-perusahaan yang bergerak di bidang keamanan komputer berlomba-lomba menawarkan jasanya. Banyak metode-metode yang digunakan oleh para pelaku kejahatan dunia maya membuat para ahli keamanan komputer melakukan penelitian secara terus-menerus, dan tak jarang para pelakunya adalah orang yang sama yang bekerja sebagai konsultan keamanan komputer, karena tidak mungkin seorang penyusup dapat masuk ke dalam sebuah sistem apabila dia tidak mengetahui caranya, dan bagaimana bisa seorang konsultan menangani kasus penyusupan sistem apabila dia tidak tahu metode apa yang digunakannya.

Dengan beranggapan bahwa pentingnya keamanan sebuah komputer terhadap aktifitas-aktifitas yang mencurigakan, perlu adanya

---

[3] http://www.fbi.gov/pressrel/pressrel01/leaveworm.htm, 14 Agustus 2001

sebuah usaha pengamanan dan pendeteksian akan bahaya yang datang baik secara fisik maupun non-fisik, namun dalam karya tulis ini akan dipertajam batasan permasalahan keamanan komputer yang di fokuskan kepada jaringan komputer, masalah keamanan terhadap jaringan komputer dianggap sangat perlu ketika komputer saling terhubung dalam sebuah sistem jaringan komputer.

Dalam skripsi ini akan dijelaskan beberapa tahapan dalam pembuatan sistem pendeteksi penyusup atau biasa dikenal dengan nama *intrusion detection system*, dimulai dari pembangunan sebuah *server* sampai dengan ke tahap konfigurasi *virtual host* sebagai alat pengelabuh dari komputer *server* yang sebenarnya, kemudian pada bab pembahasan akan menjelaskan tentang alur hidup sebuah sistem pendeteksi penyusup, cara-cara mengidentifikasi adanya aktifitas-aktifitas yang mencurigakan pada *server* dan contoh kasus dari penggunaan sistem pendeteksi penyusup, dari penjelasan latar belakang di atas maka penulis memberikan judul pada karya ilmiah ini dengan judul:

"PRARANCANGAN SISTEM PENDETEKSI PENYUSUP (INTRUSION DETECTION SYSTEM) DENGAN VIRTUAL HOST PADA SERVER"

1.2 Rumusan Masalah

Rumusan masalah dari perancangan sistem pendeteksi penyusup *(intrusion detection system)* dengan menggunakan *virtual host* pada server ini terbagi dalam dua hal, yaitu:

1. Bagaimana merancang sistem pendeteksi penyusup dengan *virtual host*?
2. Bagaimana cara mengidentifikasi adanya aktifitas-aktifitas yang mencurigakan dalam sistem pendeteksi penyusup?

1.3 Batasan Masalah

Dengan bertitik tolak rumusan masalah yang ada, maka karya ilmiah yang berjudul perancangan sistem pendeteksi penyusup *(intrusion detection system)* dengan menggunakan *virtual host* pada *server*, terdapat beberapa batasan masalah antara lain:

1. Penggunaan sistem operasi berbasis linux dengan distribusi Ubuntu versi 8.10 sebagai sistem operasi *server*
2. Perancangan sistem pendeteksi penyusup *(intrusion detection system)* dengan menggunakan *virtual host*.
3. Konfigurasi *virtual host* yang menggunakan paket program honeypot.

4. Untuk membuat *virtual host* digunakan paket program honeypot dengan versi yang terbaru, dimana honeypot ini dapat berjalan dengan baik pada ubuntu versi 8.10
5. Pengidentifikasian adanya aktifitas-aktifitas mencurigakan pada *server* dengan cara menganalisa *log* yang dihasilkan dari proses *capturing* sistem pendeteksi penyusup.

1.4 Maksud dan Tujuan

1.2.1 Maksud

Berdasarkan latar belakang yang telah diuraikan, maksud dari penulisan skripsi ini adalah merancang sebuah sistem pendeteksi penyusup *(intrusion detection system)* dengan *virtual host* pada *server*, selain itu maksud dari penyusunan skripsi ini adalah sebagai salah satu syarat dalam pencapaian gelar strata satu (S1) pada Fakultas Teknik Universitas Bhayangkara Jakarta Raya.

1.2.2 Tujuan

Menindaklanjuti maksud di atas, maka tujuan dari penulisan skripsi ini lebih mengarah kepada penerapan sistem pendeteksi penyusup dan mengidentifikasi adanya aktifitas-aktifitas

mencurigakan yang terdapat dalam komputer dengan menganalisis *virtual host* yang ada di dalam komputer *server* tersebut.

1.3 Metode Penelitian

Pada tahap penelitian sebelumnya penulis melakukan beberapa proses percobaan dalam perancangan sebuah sistem pendeteksi penyusup, tahapan-tahapan tersebut meliputi beberapa proses seperti melakukan peninjauan tentang penelitian-penelitian sebelumnya yang berkaitan dengan perancangan sebuah sistem pendeteksi penyusup dengan virtual host, tabel di bawah ini menggambarkan tentang tahapan dan jangka waktu yang dibutuhkan dalam penelitian perancangan sistem pendeteksi penyusup dengan *virtual host* pada *server*.

Tabel 1.1 Tabel Penelitian

Keterangan	Mei				Juni				Juli			
	I	II	III	IV	I	II	III	IV	I	II	III	IV
Pemilihan tema, topik dan judul												
Identifikasi kebutuhan obyektif												
Studi pustaka												
Perancangan												
Penerapan sistem												
Evaluasi												
Kesimpulan												

Dalam penyusunan skripsi perlu adanya metode-metode penelitian yang nantinya akan dijadikan bahan dalam proses penyusunan skripsi, metode penelitian yang akan digunakan dalam penulisan skripsi ini antara lain:

1.5.1 Metode Observasi

Pengertian dari metode observasi ini adalah merupakan teknik pengumpulan data dengan menggunakan indra, dimana instrument yang digunakan dalam observasi adalah panduan pengamatan dan lembar pengamatan. Metode obsevasi ini dilakukan pada minggu ketiga di bulan Juni 2009, dimana pada tahapan ini penulis melakukan perancangan sebuah sistem pendeteksi penyusup dengan membandingkan penelitian-penelitian yang sudah ada sebelumnya, kemudian hasil observasi ini akan dijelaskan secara terperinci pada bab tiga yang akan membahas mengenai tahap-tahap perancangan sistem pendeteksi penyusup dengan menggunakan *virtual host*, di mulai dari pembangunan sebuah *server* sampai dengan penyesuaian *virtual host* pada *server* sampai dengan evaluasi dari beberapa tahapan perancangan yang sudah dilakukan.

1.5.2 Studi Pustaka

Metode penelitian dengan menggunakan studi pustaka adalah metode penelitian yang digunakan dengan cara mengumpulkan buku-buku referensi dan informasi-informasi melalui internet yang berhubungan dengan penelitian yang akan dilakukan. Dalam skripsi ini metode studi pustaka akan dibahas secara terperinci pada bab dua yang berisi tentang teori-teori yang berhubungan dengan perancangan sistem pendeteksi penyusup.

1.5.3 Eksperimen

Pengumpulan data melalui pencatatan langsung dari percobaan atau pengukuran terhadap objek penelitian yang dilakukan, tahapan eksperimen dilakukan pada awal minggu pertama di bulan Juni 2009, seiring dengan proses perancangan sistem pendeteksi penyusup, dilakukan juga proses pencatantan tentang temuan permasalahan yang terjadi selama proses perancangan dan dibukukan dalam sebuah kumpulan evaluasi, dalam skripsi ini metode eksperimen akan dibahas pada bab empat, dimana dalam bab ini akan dijelaskan mengenai hasil dari

proses perancangan sistem pendeteksi penyusup seperti cara-cara mengidentifikasi adanya aktifitas-aktifitas yang mencurigakan pada sistem pendeteksi penyusup setelah dibangunnya sistem tersebut, selain itu pada bab ini juga akan diberikan contoh kasus dari serangan peretas terhadap sebuah server yang mengaplikasikan adanya sistem virtual host.

1.6 Sistematika Penulisan

Adapun sistematika penulisan karya ilmiah ini yang berjudul perancangan sistem pendeteksi penyusup *(intrusion detection system)* dengan menggunakan *virtual host* pada *server* sebagai berikut:

BAB I Pendahuluan.

Bab ini berisi tentang uraian singkat mengenai:

a. Latar Belakang.
b. Maksud dan Tujuan.
c. Rumusan Masalah.
d. Batasan Masalah.
e. Metode Penelitian.
f. Sistematika Penulisan.

BAB II Tinjauan Pustaka.

Bab ini berisi tentang uraian materi atau teori yang berhubungan dengan perancangan sistem pendeteksi penyusup *(intrusion detection system)* dengan menggunakan *virtual host*, yang di peroleh dari rujukan buku-buku atau media informasi yang terdapat pada *internet.*

BAB III Perancangan Sistem Pendeteksi Penyusup (Intrusion Detection System) Dengan Menggunakan Virtual Host Pada Server.

Bab ini berisi tentang proses perancangan objek penelitian, yaitu bagaimana cara menginstalasi sistem operasi pada *server* dan membangun sebuah *virtual host* di dalamnya dan beberapa evaluasi.

BAB IV Hasil dan Pembahasan.

Bab ini berisi tentang hasil dari perancangan objek penelitian dan pembahasan tentang temuan-temuan dalam proses perancangan, meliputi identifikasi terhadap *virtual host* dan contoh kasus serangan peretas terhadap sebuah *server*, di bab ini juga akan dijelaskan beberapa kategori sistem pendeteksi penyusup.

BAB V Kesimpulan dan Saran.

Bab ini berisi tentang kesimpulan dari proses perancangan sistem pendeteksi penyusup *(intrusion detection system)* dengan menggunakan *virtual host* pada *server,* serta saran dalam pengaplikasian *intrusion detection system* agar berjalan dengan optimal.

Daftar Pustaka.

Dalam daftar pustaka ini akan berisi beberapa referensi tentang sumber-sumber materi maupun buku-buku yang dijadikan sebagai acuan dalam penulisan karya ilmiah ini, selain itu ada juga beberapa referensi yang bersumber dari media *internet* yang dilengkapi dengan alamat situsnya.

Lampiran.

Lampiran ini berisi tentang skrip program dan cuplikan gambar *(print screen)* dari hasil perancangan *intrusion detection system* dengan menggunakan *virtual host* pada *server.*