BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Kemajuan teknologi informasi pada saat ini terus berkembang seiring dengan kebutuhan manusia yang menginginkan kemudahan, kecepatan dan keakuratan serta keamanan dalam memperoleh informasi. Oleh karena itu kemajuan teknologi informasi harus terus diupayakan dan ditingkatkan kualitas dan kuantitasnya. Salah satu kemajuan teknologi informasi di bidang transmisi pada saat ini yang berkembang selain *Fiber Optic* ialah, penggunaan perangkat *Wireless* LAN (*WLAN ; Wireless Local Area Network*), dimana perangkat *Wireless* LAN memungkinkan adanya hubungan para pengguna informasi walaupun pada saat kondisi *mobile* (bergerak), sehingga memberikan kemudahan kepada para pengguna informasi dalam melakukan aktifitasnya.

Wi-Fi (*Wireless Fidelity*) adalah istilah umum untuk peralatan *Wireless* LAN, yang juga dikenal dengan WLAN. Biasanya peralatan WiFi mengapdopsi standar keluarga IEEE 802.11, yang didukung oleh banyak *vendor*. Istilah Jaringan Nirkabel atau *Wireless* LAN adalah teknologi jaringan yang tidak menggunakan perangkat kabel yang umumnya dijumpai di dalam sebuah jaringan komputer dewasa ini. Teknologi ini sesuai dengan namanya *wireless* yang artinya tanpa kabel, memanfaatkan gelombang radio untuk melakukan interaksi atau komunikasi antar unit komputer .

Infrastruktur Jaringan Nirkabel memiliki satu masalah terbesar, terutama yang membuka akses untuk umum, seperti *hotspot*, adalah masalah pada keamanannya, dimana banyak terjadi penyerangan oleh satu atau beberapa orang penyerang (*attacker*) baik pada *server* penyedia *hotspot* atau pengguna. Dengan demikian dibutuhkan suatu taktik atau teknik pengamanan guna menanggulangi masalah tersebut.

Teknik pengamanan sistem jaringan lama adalah melakukan blokade serangan dengan *firewall*, atau mendeteksi pada saat mulai terjadi serangan dengan IDS (*Intrusion Detection Systems*). Kedua teknik ini sangat baik tapi mempunyai keterbatasan. Dengan sedikit waktu dan informasi tambahan, seorang penyerang akan dapat mempelajari untuk mengelak dari sistem blokade *firewall*. Setelah berhasil dielakkan, *firewall* tidak dapat memberikan sistem proteksi yang lebih jauh. Sementara IDS hanya akan menyediakan informasi satu kali saat sebuah serangan dimulai. Seringkali ini tidak memberikan waktu yang cukup bagi seorang *administrator* untuk mengamankan semua sistem yang terserang dikarenakan suatu serangan berada diantara paket-paket data yang sah ditambah lagi tingkat trafik jaringan yang tinggi sehingga sulit bagi IDS untuk membedakannya.

Selain *firewall* dan atau IDS, ada teknik lain yang bekerja dengan memperdaya, mengelabui dan menjebak penyerang (*attacker*) untuk masuk ke dalam sistem atau *server* palsu yang dibuat mirip dengan yang asli, yang dikenal dengan *Honeypot*.

Honeypot merupakan sebuah sistem atau komputer yang sengaja "dikorbankan" untuk menjadi target serangan dari penyerang (*attacker*). Komputer tersebut melayani setiap serangan yang dilakukan oleh *attacker* dalam melakukan penetrasi terhadap *server* tersebut. *Honeypot* akan 'menipu' atau memberikan data palsu apabila ada orang yang memiliki maksud yang tidak baik ketika ia masuk ke suatu sistem atau *server*. Secara teori, *honeypot* tidak akan mencatat trafik yang legal. Sehingga bisa dilihat bahwa yang berinteraksi dengan *honeypot* secara kebanyakan adalah *user* yang menggunakan sumber daya sistem secara *illegal*. Jadi *honeypot* seolah-olah menjadi sistem yang 'berhasil disusupi', oleh *attacker*, padahal *penyerang* tidak masuk ke sistem sebenarnya, tetapi malah masuk ke sistem yang palsu.

Salah satu *software honeypot* yang cukup terkenal dan banyak dipakai adalah *honeyd*, ia akan menjebak *attacker* dengan membuat *server-server* palsu dengan bermacam jenis sistem operasi seperti, Windows, UNIX, Linux, dan Mac OS bahkan CISCO *Router* dengan berbagai layanan (*service*) seperti, FTP, *Web Server*, dan sebagainya. Salah satu kelebihan *Honeyd* adalah mengemulasikan banyak *server* dan layanan (*service*) palsu hanya pada satu unit komputer atau *server* sehingga akan menghemat *resource*.

Jaringan nirkabel yakni, *hotspot* terutama *server* akan relatif aman dari gangguan penyerang (*attacker*) dengan cara mengelabui, menjebak dan memperdaya, dengan menerapkan sistem keamanan *honeypot* berbasis *honeyd*.

1.2. Rumusan Masalah

Adapun rumusan masalah dari latar belakang yang ada adalah menerapkan *honeypot* berbasis *honeyd* pada jaringan nirkabel (*hotspot*) guna meningkatkan keamanan pada *hotspot* dengan memonitor aktifitas penyerang (*attacker*) dan mengelabui atau menjebak, sehingga server penyedia *hotspot* terhindar dari serangan.

1.3. Batasan Masalah

Batasan masalah yang dimaksud untuk lebih mengarahkan penulis dalam pembahasan skripsi ini sehingga lebih jelas dan terarah. Dan lebih mengarahkan penulis dalam memilih dan menentukan metode yang tepat dan cepat dalam menentukan tercapainya penelitian yang penulis lakukan. Adapun batasan-batasan yang penulis lakukan meliputi ;

a. Implementasi *honeypot* ini akan diterapkan hanya pada Jaringan nirkabel (*Hotspot)* dengan skala yang kecil dengan satu buah *Access Point*.
b. *Honeyd* sebagai *honeypot* hanya akan dikonfigurasi membentuk beberapa *server* jebakan seperti ; Windows, Linux, UNIX atau Linksys *Access Point* (*Wireless Router*) dengan beberapa layanan (*service*) seperti FTP, *Web Server, Telnet* dan sebagainya.
c. Beberapa pengujian serangan terhadap *server* utama atau *server* jebakan memanfaatkan layanan-layanan yang tersedia.
d. Menganalisa *log file* yang tercatat pada *honeyd*.

1.4. Maksud Dan Tujuan

Adapun maksud dan tujuan diadakan penelitian ini adalah,

Tujuan secara khusus ;

a. Penelitian ini dibuat sebagai syarat kelengkapan akademik untuk memperoleh gelar Sarjana S1 pada Sekolah Tinggi Manajemen Informatika dan Komputer STMIK "AMIKOM" Yogyakarta.

Tujuan secara umum ;

a. Instalasi jaringan nirkabel (*hotspot*) yang dilengkapi *honeyd* sebagai *software honeypot* pada distro Ubuntu 9.04.
b. Konfigurasi *honeyd* untuk membentuk beberapa *server* jebakan dan layanan (*service*).
c. Memonitor dan membaca *log file* dari *honeyd* sehingga diketahui asal penyerang (*attacker*).

1.5. Metodologi Penelitian

Metode yang penulis lakukan bertujuan agar hasil dari penelitian dan analisa dapat lebih terarah serta data yang diperoleh lebih akurat. Kelengkapan data yang diperoleh dapat memberikan kontribusi bagi penulis dalam menyusun skripsi ini dan memberikan waktu yang lebih singkat. Adapun beberapa metode yang penulis lakukan dalam pengumpulan data terdiri dari ;

a. Metode observasi.

   Pengumpulan data dengan pengamatan secara langsung pada objek yang diteliti untuk memperoleh informasi yang tepat dan sistematis. Meliputi instalasi, konfigurasi, *tools* yang dipakai dan pengujian koneksi terhadap internet.

b. Metode *interview* atau wawancara.

   Pengumpulan data dengan mengadakan tanya jawab secara langsung dengan responden atau sumber data yang dianggap perlu, bahkan penulis langsung menanyakan hal yang dianggap tidak diketahui dengan mengikuti *mailing list* dan *forum*.

c. Metode kepustakaan.

   Pengumpulan data dengan cara membaca berdasarkan kepustakaan dari buku, jurnal maupun makalah yang mana dimaksudkan untuk mendapatkan konsep teori mengenai masalah yang diteliti serta mencari sumber data di internet dan perpustakaan.

1.6. Sistematika Penulisan

Sistematika penulisan yang disusun oleh penulis akan memuat uraian secara garis besar isi dari skripsi tiap-tiap babnya, yaitu sebagai berikut ;

BAB I Pendahuluan

Bab Pendahuluan berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan, metodologi dan sistematika penulisan.

BAB II Landasan Teori

Bab landasan teori berisi tinjauan pustaka dari penelitian-penelitan sebelumnya dan teori yang mendasari penyusunan skripsi ini. Adapun yang dibahas dalam bab ini adalah teori yang berkaitan jaringan nirkabel terutama *Hotspot*, standar IEEE 802.11 (WiFi), konsep dari *honeypot* dan *honeyd*.

BAB III Metode Penelitian

Pada bab ini akan diuraikan detail-detail dari penelitian yang penulis lakukan. Mencakup subjek penelitian, alat penelitian dan konsep serta rancangan sistem jaringan yang akan digunakan berikut proses instalasinya.

BAB IV Hasil Dan Pembahasan

Pada bab ini akan diuraikan hasil perancangan sistem yang telah dilakukan dan pembahasannya. Mencakup hasil yang ditemui pada penelitian, pengujian-pengujian yang dilakukan pada konfigurasi *honeyd* yang telah diterapkan dan dampak yang terjadi pada penyerang (*attacker*).

BAB V Penutup

Bab Penutup berisi Kesimpulan dari penelitian dan Saran bagi penelitian selanjutnya.

1.7. Jadwal Pembuatan Dan Penyusunan Skripsi

Untuk memperlancar kegiatan penelitian ini agar dapat terencana dan tepat waktu, maka penulis membuat suatu rencana jadwal kegiatan agar mencapai target yang dibutuhkan. Adapun rencana kegiatan diuraikan sebagai berikut:

Tabel 1.1. Jadwal Pembuatan dan Penyusunan Tugas Skripsi

Uraian Kegiatan	MEI				JUNI 2009				JULI 2009			
	Minggu ke				Minggu ke				Minggu ke			
	1	2	3	4	1	2	3	4	1	2	3	4
Persiapan												
Pengumpulan Data												
Perancangan / Desain												
Implementasi												
Uji coba dan Analisa												
Pembuatan Laporan												