BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi di dunia yang semakin pesat mempermudah manusia untuk melakukan banyak hal hanya dengan internet. Efisiensi waktu dan tenaga yang disediakan oleh internet membuat orang dengan mudah melakukan banyak hal dalam satu waktu, seperti berbelanja, berhubungan dengan orang-orang terdekatnya, memantau keadaan lalu lintas menuju tempat yang akan dituju, mengecek surat elektronik, dan lain-lain.

Semakin murahnya dan cepatnya teknologi internet mendorong orang untuk terhubung ke dalamnya secara tidak langsung. Dengan semakin banyaknya individu maupun korporat yang memanfaatkan teknologi internet, komunitas dunia maya semakin besar dan berkembang. Sama halnya dengan tatanan sosial masyarakat yang ada di dunia nyata, isu keamanan adalah hal yang sangat penting dalam suatu tatanan masyarakat. Keamanan dalam dunia internet adalah suatau hal yang krusial, pemanfaatan internet sudah mencapai titik yang sangat penting dalam pembangunan infrastruktur sebuah perusahaan ataupun pemerintah dan negara. Komunikasi antar kantor cabang yang berjauhan, toko *on-line*, bursa saham, *on-line banking*, pelayanan masyarakat, pajak *on-line*, adalah sedikit contoh dari pemanfaatan internet yang berguna.

Keamanan, kerahasiaan data khususnya pada sebuah dunia internet menjadi mahal harganya jika dihadapkan dengan isu *hacking* atau *cracking*. *Hacking* atau *cracking* secara umum adalah kegiatan sesorang atau lebih yang mengambil alih akses kontrol sebuah atau beberapa komputer secara paksa, secara sembunyi-sembunyi, atau terang-terangan atau melakukan serangan-serangan yang bersifat merusak atau melumpuhkan sebuah sistem teknologi informasi. Dengan pengetahuan dan pengalaman dan mendalam pada ilmu komunikasi data, dan sistem operasi umumnya dan teknik-teknik *hacking* khususnya, seseorang dapat menggunakan kelemahan sebuah infrastruktur sistem teknologi informasi tertentu untuk mendapatkan data-data yang sensitif atau mendapatkan hak akses tertinggi dalam sebuah infrastruktur tanpa diketahui. Ini tentu sangat tidak diinginkan oleh pihak manapun, oleh karena itu pencegahan harus dilakukan sebelum hal tersebut terjadi.

Tidak ada yang sempurna di dunia ini, hal itu juga berlaku dalam sistem teknologi informasi manapun yang paling mahal dan canggih sekalipun. Oleh karena itu pengetahuan akan kelemahan sebuah sistem menjadi bahan dasar yang wajib dipelajari untuk mencegah serangan-serangan dalam jaringan internet. Untuk melakukan pencegahan terhadap serangan *hacker* dan *cracker* banyak hal yang dapat dilakukan, misalnya menutup celah keamanan suatu sistem atau menggunakan *firewall*.

Selain kedua konsep keamanan di atas, ada konsep lain yang lain dari biasanya yaitu *Honeypot*. *Honeypot* adalah sebuah seistem yang mengemulasikan sebuah sistem operasi tertentu yang seakan-akan lemah dan mudah dapat

dipenetrasi dengan mudah. Konsep ini bisa dibilang tidak biasa, karena "membiarkan" seorang hacker atau cracker untuk mempenetrasi sebuah sistem, agar dapat mempelajari perilaku penyerang, jenis serangan, dan asal serangan.

Dengan meningkatnya jumlah serangan-serangan yang terjadi di dunia internet, solusi dengan menggunakan *Honeypot* ini dapat menjadi pilihan untuk mempelajari dan mengatasi serangan yang terjadi di Indonesia. Skripsi ini ditujukan untuk mempelajari dan menganalisa pola serangan yang terjadi di jaringan internet untuk dapat diantisipasi ke depannya.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas maka penulis merumuskan permasalahan sebagai berikut :

1. Bagaimana menganalisa serangan-serangan yang umum terjadi dan darimana asalnya.
2. Bagaimana menganalisa tren dari malware-malware yang diperoleh.
3. Bagaimana meningkatkan kemanan dari sistem yang digunakan dari hasil analisa.

1.3 Batasan Masalah

Pada pembuatan skripsi ini penulis membatasi ruang lingkup penulisan meliputi :

1. Melakukan analisa dan identifikasi dari hasil log Honeypot.

2. Membatasi analisa dan identifikasi serangan ke port-port yang umum digunakan pada sistem operasi dan aplikasi-aplikasi yang berhubungan dengan internet.
3. Program yang penulis gunakan adalah Nephentes untuk Linux.

1.4 Maksud dan Tujuan Penelitian

Maksud dalam penulisan skripsi ini adalah sebagai berikut:

1. Sebagai syarat untuk menyelesaikan program studi Strata-1 Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
2. Menerapakan ilmu dan teori-teori selama mengikuti pendidikan ke dalam aplikasi nyata secara praktis guna membantu dan mendukung kemampuan beraktualisasi dalam penerapan ilmu di dunia nyata.

Tujuan dalam penulisan skripsi ini adalah sebagai berikut:

1. Mengimplementasi sistem *honeypot* di lingkungan STMIK AMIKOM Yogyakarta.
2. Dapat mengenali pola serangan di jaringan internet di lingkungan STMIK AMIKOM Yogyakarta.

1.5 Metode Penelitian

Metodologi penelitian yang digunakan untuk memenuhi bahan atau sumber yang diperlukan dalam penulisan skripsi ini yaitu :

1. Studi Pustaka

Dengan metode ini penulis melakukan pencarian dan pembacaan tentang buku-buku, majalah atau referensi yang berhubungan dengan *local area network*, internet, *hacking methodology*, *firewall*, *honeypot* dan lain-lain.

2. Studi Lapangan

Dalam penelitian lapangan penulis melakukan penelitian dan analisa tentang celah-celah kemanan yang sering diekploitasi, tipe-tipe Trojan dan *malware*, dan tipe-tipe serangan yang umum di internet.

3. Percobaan

Dalam percobaan penulis melakukan proses instalasi honeypot di sistem operasi Linux dan menganalisa hasilnya.

1.6 Sistematika Penelitian

Penyusunan skripsi ini dibagi atas 5 bab, tiap bab terdiri dari beberapa sub bab. Untuk memperjelas penyusunan skripsi ini, maka secara garis besar sistematika penulisan dibagi menjadi :

BAB I PENDAHULUAN

Merupakan uraian umum yang memuat mengenai hal-hal yang menjadi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, serta sistematika penulisan.

BAB II LANDASAN TEORI

Merupakan pembahasan secara jelas tentang teori-teori dasar yang relevan dengan masalah pokok yang akan dikaji, pengertian-pengertian yang berhubungan dengan jaringan *LAN, Internet, hacking* kemanan internet dan *Honeypot*.

BAB III RANCANG BANGUN SISTEM HONEYPOT BERBASIS NEPENTHES

Merupakan uraian umum mengenai metode yang digunakan penulis dalam melakukan perancangan untuk pengimplementasian terhadap sistem yang akan dibangun.

BAB IV HASIL DAN PEMBAHASAN

Pembahasan yang dibahas pada bab ini adalah mengenai hasil dan implementasi sistem dan melakukan pembahasan dari log yang dihasilkan

BAB V PENUTUP

Merupakan bagian akhir dari penulisan skripsi yang berisi uraian kesimpulan dari seluruh bahasan dan saran-saran yang dianggap penting dan perlu ditekankan untuk menyempurnakan penulisan skripsi ini.

1.7 Rencana Kerja

Rencana kerja dalam penyusunan skripsi ini, dapat dilihat pada tabel di bawah ini.

Tabel 1.1 Rencana Kerja

No	Kegiatan	Bulan (2010)							
		September		Oktober				November	
		III	IV	I	II	III	IV	I	II
1	Identifikasi Masalah								
2	Pengumpulan Data								
3	Implementasi Sistem								
4	Monitoring Sistem								
5	Penyusunan Laporan								