BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan merupakan segala aktivitas pengamanan suatu jaringan yang bertujuan untuk melindungi semua data dari penggunaan yang tidak sah atau berbahaya dalam jaringan tersebut [1]. Perkembangan teknologi terutama pada teknologi Internet dan Komputer, telah mempengaruhi kehidupan kita sehari-hari. Mulai dari cara berkomunikasi, mencari informasi, bermain, bahkan melakukan pekerjaan rutin sehari-hari [2]. Dengan meningkatnya jumlah pemakaian jaringan yang signifikan, maka serangan dan ancaman dan resiko jahat pun semakin meningkat. Salah satunya yaitu intrusi, didefinisikan sebagai serangkaian tindakan yang berusaha untuk mengambil dan merusakan integritas (*integrity*), kerahasiaan (*confidentiality*), atau ketersediaan sumber daya (*availability*) dalam suatu jaringan [3]. Serangan dan ancaman aman terbagi menjadi 2 macam, yaitu eksternal dan internal. Serangan dan ancaman internal terjadi apabila ada seseorang dari dalam jaringan bertanggung jawab atas terjadinya serangan dan ancaman, karena seseorang dalam jaringan internal memiliki akses langsung ke dalam jaringan gedung dan perangkat infrastrukturnya, juga memiliki pengetahuan tentang jaringan perusahaan/organisasi, sumber daya, dan data rahasia. Perusahan/organisasi yang mengalami kebocoran keamanan terjadi karena serangan dan ancaman internal yang menyebabkan kerugian aset yang besar. Serangan dan ancaman internal ini dapat berupa malware, ddos, pencurian data, *unauthorized access*, penggunaan *resource* perusahaan secara illegal [4]. Sedangkan serangan dan ancaman eksternal terjadi apabila ada seseorang yang memanfaatkan kerentanan dalam jaringan atau perangkat komputer, atau menggunakan rekayasa sosial untuk mendapatkan akses masuk kedalam jaringan [5]. Permasalahan saat ini yaitu, tidak sedikit organisasi yang hanya memiliki keamanan jaringan sebatas *Firewall* saja yang hanya mengatasi serangan dan ancaman eksternal, sehingga resiko akan terkena serangan dan ancaman internal sangatlah besar.

Untuk mencegah resiko akan terkena serangan dan ancaman internal, maka perlu suatu solusi untuk melindungi data didalam suatu jaringan, salah satu yang dimanfaatkan untuk sistem keamanan jaringan yaitu *honeypot. Honeypot* merupakan perangkap yang ditetapkan untuk mengenali, mengalihkan atau dalam beberapa cara menyeimbangkan upaya pada pemanfaatan data yang tidak disetujui [6]. *Honeypot* didesain menyerupai sistem yang asli dan dibuat dengan tujuan untuk diserang atau disusupi sehingga sistem yang asli tetap aman dan terhindar dari serangan [7]. Perbedaan dan keunggulan *honeypot* dengan sistem keamanan jaringan yang lain yaitu *honeypot* memiliki respon deteksi yang cepat terhadap adanya serangan dan ancaman yang masuk kedalam sistem [8].

Harapannya dengan adanya sistem keamanan jaringan dengan menggunakan *honeypot* ini, layanan jaringan dapat terhindar dari berbagai serangan dan ancaman, juga dapat mengumpulkan informasi mengenai penyerang yang meliputi identitas dan aktivitas yang dilakukan oleh penyerang dalam melakukan serangan ke layanan jaringan. Dari informasi inilah penyedia layanan nantinya dapat meningkatkan pengamanan pada layanan yang dimilikinya.

1.2 Maksud dan Tujuan

Adapun maksud dari penelitian ini adalah menerapkan dan menganalisis sistem keamanan jaringan menggunakan sistem *honeypot*.

Sedangkan tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut:

1. *Honeypot* dapat mendeteksi adanya aktivitas serangan ke dalam sistem keamanan jaringan yang telah dibuat dengan memberikan *log* secara *real time.*
2. Dapat mendeteksi serangan terhadap *host* yang ada di dalam jaringan.
3. Hasil *log* dapat dilihat di dalam *web interface* dengan bentuk grafik.

1.3 Batasan Masalah

Agar penelitian ini mengarah pada pembahasan yang diharapkan dan terfokus pada pokok permasalahan yang ditentukan, maka diperlukan batasan masalah dalam penelitian ini. Batasan masalah pada penelitian ini ditentukan dalam beberapa hal, sebagai berikut:

1. *Honeypot* lebih difungsikan untuk mendeteksi jenis serangan *Flooding Attack* dengan tujuan *port* TCP/IP yaitu *port* TCP dan UDP.
2. Menggunakan *honeypot* dengan level *low-interaction*.

1.4 Metode Penelitian

Untuk memudahkan di dalam pelaksanaan penelitian ini, diperlukan sebuah metode penilitian yang akan diselesaikan secara bertahap. Adapun tahapannya yaitu sebagai berikut:

1. Studi Pustaka

Metode pengumpulan data dengan cara mencari referensi, membaca, dan mempelajari buku-buku yang berkaitan dengan masalah dalam pengerjaan penelitian ini.

2. Perancangan

   Melakukan perancangan untuk simulasi sistem yang akan dibangun berdasarkan data dan bahan yang telah didapat.

3. Implementasi

   Implementasi adalah tahap pembuatan simulasi sistem keamanan jaringan yang di rancang pada sistem operasi Linux.

4. Pengujian dan Analisa

   Pada tahap ini akan dilakukan pengujian terhadap simulasi sistem yang telah dibuat, data hasil pengujian yang diperoleh akan dianalisis sehingga dapat ditarik suatu kesimpulan.

5. Kesimpulan

   Mengambil data-data yang diperlukan ketika pengujian, guna membuat hasil analisa serta laporan dalam pembangunan simulasi sistem tersebut.

1.5 Sistematika Penulisan

Dalam mempermudah pembahasan dan pemahaman teori, serta dalam memberi gambaran mengenai skripsi ini, maka akan diuraikan sistematika penulisan skripsi ini.

BAB I PENDAHULUAN

Menjelaskan tentang latar belakang masalah, masalah dan tujuan, batasan masalah, metode penelitian, serta sistematika penulisan.

BAB II TEORI PENUNJANG

Menjelaskan teori-teori pendukung yang berhubungan dengan penelitian, diantaranya teori dasar jaringan komputer, sistem keamanan jaringan, pengertian dan klasifikasi *honeypot*, pengertian sistem operasi Linux, model penyerangan jaringan dan penjelasan *VMWare Workstation*.

BAB III PERANCANGAN SISTEM

Menjelaskan tentang langkah-langkah merancang sebuah simulasi sistem keamanan jaringan menggunakan *honeypot* pada sistem operasi Linux, topologi jaringan simulasi yang akan dirancang, analisis kebutuhan sistem dan konfigurasi *honeypot*.

BAB IV PENGUJIAN DAN ANALISIS

Menjelaskan perihal hasil dari pengujian yang telah dilakukan, diantaranya adalah dengan mengirimkan perintah *flooding* menggunakan *tools* Zenmap, LOIC dan *Packets Generator* serta analisa dari hasil pengujian tersebut.

BAB V SIMPULAN DAN SARAN

Memuat Kesimpulan dari hasil pengujian dan analisa yang didapat dari BAB IV dan saran yang memuat tentang hal – hal yang perlu dikembangkan lebih lanjut ataupun sebagai pembanding dari hasil yang sebelumnya telah didapat.