BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi infromasi pada jaringan komputer saat ini sudah semakin maju dan berkembang serta dapat di aplikasikan di berbagai bidang. Karena alasan tersebut membuat banyak pihak saat ini sangat bergantung kepada sistem jaringan komputer, namun sistem jaringan komputer masih miliki beberapa masalah yang serius. Salah satunya adalah terkait faktor keamanan. Faktor keamanan menjadi begitu penting di karenakan tidak semua data atau informasi yang tersedia bersifat terbuka untuk umum dan tak semua orang juga berhak untuk mengaksesnya. Oleh karena itu, informasi akan menjadi aset yang sangat berharga baik bagi perseorangan, pemerintah maupun pihak swasta. Informasi memiliki nilai dan harus dilindungi, sehingga menjadi penting bagi individu untuk melakukan perlindungan terhadap informasi. [10]

Informasi sangat berharga karena jika suatu informasi tersebut berada di tangan pihak yang tidak berhak bisa disalahgunakan. Salah satu contoh nya ketika data pada suatu perusahaan bisa diambil oleh pesaing bisnis dapat digunakan sebagai alat untuk menjatuhkan perusahaan tersebut. Namun sampai saat ini masih banyak organisasi atau perusahaan belum sepenuhnya menyadari pentingnya perlindungan informasi, karena masih banyak yang menganggap informasi bukan bagian dari aset.[6]

Menurut G.J Simons keamanan informasi adalah bagaimana usaha untuk dapat mencegah penipuan (*cheating*) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik. Aspek-aspek yang harus dipenuhi dalam suatu sistem untuk menjamin keamanan informasi adalah informasi yang diberikan akurat dan lengkap (*right information*), informasi dipegang oleh orang yang berwenang (*right people*), dapat diakses dan digunakan sesuai dengan kebutuhan (*right time*), dan memberikan informasi pada format yang tepat *(right form*). Dalam membuat program keamanan informasi ada prinsip dasar yang harus dipenuhi agar sistem tersebut handal. Prinsip dasar tersebut adalah:[6]

Kerahasiaan artinya informasi dijamin hanya tersedia bagi orang yang berwenang sehingga pihak yang tidak berhak tidak bisa mengakses informasi. Contoh kerahasiaan adalah seorang administrator tidak boleh membuka atau membaca email milik pengguna. Selain itu kerahasiaan harus menjamin data-data yang harus dilindungi penggunaan dan penyebarannya baik oleh pengguna maupun administrator, seperti nama, alamat, tempat tanggal lahir, nomor kartu kredit, penyakit yang diderita, dan sebagainya.[6]

Integritas artinya informasi dijaga agar selalu akurat, untuk menjaga informasi tersebut maka informasi hanya boleh diubah dengan izin pemilik informasi. Virus *trojan* merupakan contoh dari informasi yang integritasnya terganggu karena virus telah mengubah informasi tanpa izin. Integritas informasi ini dapat dijaga dengan melakukan enkripsi data atau membuat tanda tangan *digital (digital signature).*

Ketersediaan artinya adanya jaminan ketika pihak berwenang membutuhkan informasi, maka informasi dapat diakses dan digunakan. Hambatan dalam ketersediaan ini contohnya adalah adanya *Denial of Service Attack (DoS). DoS* merupakan serangan yang ditujukan ke server, di mana banyak sekali permintaan yang dikirimkan ke server dan biasanya permintaan tersebut palsu yang menyebabkan server tidak sanggup lagi melayani permintaan karena tidak sesuai dengan kemampuan sehingga server menjadi down bahkan error.

Salah satu alat bantu yang dapat digunakan untuk meningkatkan sistem keamanan komputer adalah *Honeypot*. Dengan menggunakan *Honeypot* kita dapat merekam segala aktivitas ilegal yang di lakukan oleh penyerang dapat digunakan oleh administrator sebagai informasi tambahan tentang penyerangan untuk menganalisis serta mempelajari aktivitas-aktivitas yang cenderung membahayakan sistem [4].

Karena menjaga sistem keamanan sangat penting, penulis ingin melakukan simulasi pengamanan jaringan pada suatu jaringan komputer. Hal ini di lakukan agar menjaga segala informasi yang ada pada server. Maka di perlukan sebuah *Dionaea Honeypot* untuk meningkatkan kemanan jaringan dari serangan orang yang tidak memiliki akses.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang, maka rumusan masalah pada penelitian ini adalah sebagai berikut.

1. Bagaimana melakukan rancang bangun simulasi jaringan sistem *dionaea honeypot* yang untuk keamanan suatu jaringan komputer?
2. Bagaimana efektifitas dari sistem *honeypot* di dalam menangkap aktifitas serangan yang dilakukan?

1.3 Tujuan Penelitian

Kegiatan penelitian ini memiliki tujuan yang ingin dicapai yaitu:

1. Melakukan simulasi jaringan *dionaea honeypot server* untuk keamanan suatu jaringan komputer.
2. Menguji dan memastikan *dionaea* dapat memproteksi suatu jaringan komputer dari serangan-serangan jaringan.

1.4 Manfaat Penelitian

Manfaat dari kegiatan penelitian ini adalah sebagai berikut.

1. Menambah wawasan tentang keamanan jaringan.
2. Peneliti dapat membuktikan penerapan dionaea untuk keamanan sistem jaringan.
3. Peneliti dapat mengetahui sejauh mana kemampuan Dionaea dalam menangkap serangan.
4. Menghasilkan Karya Tulis yang dapat menjadi acuan dalam merancang & mengimplementasikan honeypot

1.5 Batasan Masalah

Batasan masalah dari kegiatan penelitian ini adalah sebagai berikut.

1. Sistem *honeypot* pada penelitian ini diimplementasikan pada *operating system* berbasis *linux.*
2. *Implementasi* dilakukan secara simulasi dengan menggunakan *virtual box.*
3. Pengujian dilakukan secara simulasi menggunakan perangkat lunak pihak ketiga yang memiliki fungsi serangan jaringan *port scanning, exploit, sql injection*

1.6 Sitematika Penulisan

Semua kegiatan yang mendukung Tugas Akhir ini ditulis dengan sistematika sebagai berikut :

Bab I : PENDAHULUAN

Bab ini berisi latar belakang dari penulisan proposal tugas akhir, perumusan masalah tujuan dan manfaat penelitian, batasan masalah dan sistematika dari penulisan proposal tugas akhir ini.

Bab II : LANDASAN TEORI

Bab ini berisikan mengenai pembahasan teori yang diperoleh dari buku-buku literatur ataupun berbagai macam refernsi yang berkaitan tentang implementasi *Honeypot* menggunakan *Dionaea*.

Bab III : METODOLOGI PENELITIAN

Bab ini berisikan tentang tahapan yang dilakukan dalam implementasi jaringan keamanan menggunakan *Honeypot*, dari mulai persiapan *Hardware* dan *Software*,

Bab IV : ANALISIS KEBUTUHAN DAN PERANCANGAN

Bab ini berisikan analisa kebutuhan yang diperlukan untuk melakukan simulasi Dionaea dan perancangan simulasi jaringan yang terimplementasi *Dionaea Honeypot*.

Bab V : IMPLEMENTASI SISTEM

Bab ini berisikan proses implementasi dari *Dionaea* dengan diuji serangan *port scan*, *metaspoilt* dan *SQL Injection* untuk melihat tingkat efektifitas dari *Dionaea*. Dimana hasil pengujian akan dianalisa untuk mendapatkan kesimpulan.

Bab VI : KESIMPULAN DAN SARAN

Bab yang berisikan kesimpulan hasil dari kegiatan penelitian dan saran untuk kegiatan penelitian lain dengan topik yang sama