BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Saat ini istilah *Cloud Computing* seringkali terdengar dan dapat dibaca di internet. Bahkan tanpa disadari masyarakat Indonesia seringkali menggunakan layanan berbasis *Cloud Computing*, misalkan saat menggunakan layanan email, layanan *streaming* dan sebagainya. Demikian pula pada pmerintahan ataupun industri swasta, banyak beralih ke layanan *Cloud*. [1]

Di dalam draftnya yang berjudul *The NIST Definition Of Cloud Computing*. *Peter Meel dan Timothy Grance* mendefinisikan *Cloud Computing* sebagai sebuah model yang memungkinkan adanya penggunaan sumber daya secara bersama-sama dan mudah, menyediakan jaringan akses dimana-mana, dapat dikonfigurasi, dan layanan yang digunakan sesuai keperluan. [1]

Dibalik semua kemudahannya, ternyata teknologi ini memiliki beberapa kelemahan, yaitu di bidang keamanan. Misalnya saja pembobolan dengan metode serangan *brute-force*. Secara sederhana metode ini adalah metode dengan menebak *password* dengan mencoba semua kombinasi karakter yang mungkin terjadi.

Dari uraian diatas, maka dibuatlah sebuah sistem keamanan jaringan menggunakan *Honeypot* yang dapat menganalisis serta mengumpulkan informasi identitas serta aktifitas yang dilakukan oleh penyerang. *Honeypot* dapat

mengalihkan perhatian *penyerang* dengan berpura-pura menjadi *server* asli sehingga terjadi interaksi sementara bagi host yang melakukan serangan. Informasi yang terkumpul dapat digunakan oleh penyedia layanan dalam meningkatkan sistem pengamanan pada infrastruktur *cloud computing*.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan, maka dapat dirumuskan masalah sebagai berikut :

1. Bagaimana mendeteksi serangan *brute-force* pada *cloud computing?*
2. Bagaimana merancang dan membangun sistem *honeypot* sebagai pendeteksi serangan paket *brute-force* pada *cloud computing*?

1.3. Batasan Masalah

Berdasarkan identifikasi masalah di atas, perlu adanya batasan agar permasalahan yang akan dibahas menjadi jelas serta tidak menyimpang, maka dibuat batasan sebagai berikut:

1. Penelitian ini hanya membahas implementasi *honeypot* untuk analisa serangan *brute-force*.
2. Ruang lingkup jaringan yang digunakan adalah lokal di jaringan *virtual machine* menggunakan *software Oracle Virtual Box*.
3. Layanan *cloud computing* pada tingkat *IaaS (Infrastructure as a Service)*.
4. Dalam pembuatan *cloud computing* menggunakan *software Proxmox*.

5. Sistem Operasi yang digunakan untuk *server* adalah *Debian*. Untuk klien dan intruder menggunakan sistem operasi *Linux Mint*.
6. *Service Honeypot* yang digunakan adalah *Kippo* dan divisualisasikan menggunakan *Kippo-Graph*

1.4. Tujuan Penelitian

Tujuan penelitian ini adalah untuk merancang sistem *honeypot* untuk mendeteksi serangan *brute-force* pada *cloud computing* serta menganalisa tingkat keberhasilan dan akurasi sistem *honeypot* dalam mendeteksi serangan *brute-force* pada *cloud computing*.

1.5. Manfaat Penelitian

Dengan dirancangnya sistem keamanan jaringan menggunakan *honeypot* untuk mendeteksi serangan *brute-force* pada *cloud computing*, diharapkan dapat memberikan manfaat sebagai berikut:

a. Bagi Penulis
   - Menambah wawasan pengetahuan, pemikiran dan pengalaman dalam bidang Teknik Informatika, khususnya di bidang keamanan jaringan untuk mendeteksi serangan pada jaringan komputer.
   - Mengetahui *tool* pada *honeypot* dalam mendeteksi serangan *brute-force*

b. Bagi Admin Jaringan
   - Mempermudah *admin* jaringan dalam mendeteksi serangan *brute-force* pada *cloud computing*, serta menangkalnya.

- Membantu *admin* jaringan komputer untuk mempersiapkan keamanan jaringan pada *cloud computing*.

c. Bagi Masyarakat

- Berperan dalam pengembangan sumber daya manusia serta pendidikan mengenai teknologi khususnya keamanan jaringan.
- Sebagai referensi penelitian-penelitian berikutnya yang membahas mengenai keamanan jaringan.

1.6. Metodologi Penelitian

Metode penelitian dan pengembangan sistem yang dilakukan untuk menyelesaikan skripsi ini adalah :

a. Analisis

Penulis melakukan analisis berdasarkan data log pertama dan kedua. Data pertama diambil dari hasil serangan ke *cloud computing*. Setelah data pertama didapat maka penulis menyiapkan *honeypot* dan mengimplementasikannya. Proses selanjutnya penulis akan memulai skenario penyerangan terhadap cloud computing lalu mengumpulkan data itu dan membandingkannya dengan data sebelumnya.

b. Desain

Membuat arsitektur *cloud computing*, membuat sistem kemanan jaringannya dan metode penyerangan aplikasi yang digunakan.

c. Implementasi dan *Testing*

Langkah selanjutnya adalah menerapkan metode serta pola serangan ke *cloud computing* yang telah diberikan sistem keamanan *honeypot*. Dari hasil serangan tersebut penulis akan mengetahui seberapa efektif sistem keamanan *honeypot* dalam melindungi *cloud computing* terhadap serangan *brute-force*.

1.7. Sistematika Penulisan

Untuk memudahkan dalam memahami dan menyusun tiap bab dalam penulisan skripsi ini, maka dijabarkan sistematika penulisan sebagai berikut:

BAB I : PENDAHULUAN

Pada bab ini merupakan bagian pengantar dari pokok permasalahan yang dibahas dalam skripsi ini, yaitu serangan *brute-force*, pola serangannya, dan bagaimana penulis merancang dan membangun system keamanan yang dapat mendeteksi dan menangkal serangan tersebut. Adapun yang dibahas memuat latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II : LANDASAN TEORI

Pada bab ini akan diuraikan tentang tinjauan dari beberapa literatur, yang menjelaskan tentang teori-teori yang terkait dengan permasalahan yang diambil, serta penjelasan mengenai

software dan *hardware* yang digunakan untuk keperluan penelitian.

BAB III : PERANCANGAN DAN ANALISIS

Pada bab ini akan membahas tentang perancangan *cloud computing*, perancangan arsitektur keamanan jaringan, metode penyerangan serta analisis *honeypot* terhadap serangan *brute-force tersebut.*

BAB IV : ANALISIS DAN PEMBAHASAN

Bab ini merupakan tahapan yang penulis lakukan dalam membuat *cloud computing*, keamanan jaringan, penerapan sistem keamanan ke *cloud computing* dan melakukan uji serangan terhadap *cloud computing*, baik sebelum dan sesudah implementasi sistem keamanan.

BAB V : PENUTUP

Pada bab ini memuat tentang kesimpulan dan saran. Kesimpulan berisi rangkuman singkat dari hasil pembahasan masalah. Sedangkan saran berisi harapan pengembangan sistem bagi sistem keamanan yang telah dibuat.