BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Keamanan menjadi konsentrasi dan fokus utama seiring dengan ketergantungan masyarakat akan teknologi informasi. Ancaman keamananpun sangat beragam, seperti ; *virus, worm, malware, backdoor, shell, denial of service* yang menyebabkan *server* akan mati dan tidak dapat beroperasi lagi sehingga otomatis tidak dapat memberikan pelayanan. Berbagai ancaman keamanan teknologi informasi dapat diminimalkan dengan memaksimalkan identifikasi celah keamanan sedini mungkin.

Kombinasi dan perpaduan keamanan *software* dan *hardware* merupakan solusi kemanan teknologi informasi yang komprehensif. Implementasi sistem *honeypot* merupakan salah satu solusi keamanan yang komprehensif. *Honeypot* adalah sistem yang dibuat seperti desain sistem aslinya agar sengaja diserang atau disusupi, sehingga informasinya dapat digunakan untuk melakukan tindakan pencegahan selanjutnya.

Cloud computing (komputasi awan) merupakan salah satu teknologi yang saat ini sedang banyak dikembangkan dan digunakan oleh perusahaan-perusahaan yang membutuhkan sumber daya komputasi yang besar dan efisien. Seiring perkembangan teknologi tersebut maka ancaman keamanan pada layanan *cloud computing* semakin meningkat. Ancaman keamanan yang paling sering digunakan oleh penyerang adalah *malware*. Salah satu tindakan pengamanan yang dapat dilakukan yaitu dengan menggunakan *honeypot*. *Honeypot* merupakan salah satu

teknologi atau sistem keamanan yang dapat memenuhi ketiga konsep keamanan teknologi informasi yaitu pencegahan *(prevention)*, deteksi *(detection)*, dan merespon *(respond)*. *Honeypot* dapat menangkap *malware* yang masuk ke jaringan, serta menangkap informasi mengenai identitas dan aktifitas yang dilakukan oleh penyerang yang kemudian akan digunakan oleh penyedia layanan *cloud computing* dalam meningkatkan sistem pengamanan.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah bagaimana mengamankan sebuah jaringan pada *cloud computing* dengan *honeypot* dari serangan *malware*.

1.3. Batasan Masalah

Beberapa batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut.

1. Penelitian ini hanya membahas implementasi *honeypot* untuk identifikasi serangan *malware*.
2. Ruang lingkup jaringan yang digunakan adalah jaringan *virtual machine* menggunakan *software VMware vSphere Hypervisor 6.0*.
3. Sistem operasi yang digunakan adalah *CentOS-7-x86_64-Minimal-1511*.
4. *Dionaea* digunakan untuk mendeteksi serangan *malware*.
5. Layanan *cloud computing* pada tingkat *IaaS (Infrastructure as a Service)*.
6. Dalam membuat *cloud computing menggunakan software Apache CloudStack 4.8.0*.

7. Menggunakan aturan dalam *firewall* untuk mengarahkan serangan ke *honeypot*.
8. Pengujian serangan *malware* menggunakan *exploit* dari *tool metasploit*.
9. Data *malware* berasal dari *website* virustotal.com.

1.4. Maksud dan Tujuan Penelitian

Tujuan dari penelitian ini dimaksudkan untuk menganalisa , mendesain, dan mengintegrasikan antara aplikasi *Dionaea* dan aplikasi *honeypot* pada layanan *cloud computing* sehingga sistem layanan *cloud computing* akan mempunyai kemampuan.

1. Mencegah serangan *malware* pada jaringan layanan *cloud computing*.
2. Mendeteksi serangan *malware* pada jaringan layanan *cloud computing*.
3. Sistem layanan *cloud computing* dapat merespon langsung serangan *malware*.
4. Sistem dapat menangkap informasi mengenai identitas dan aktifitas yang dilakukan oleh penyerang jaringan layanan *cloud computing*.
5. Memudahkan penyedia layanan *cloud computing* dalam meningkatkan sistem pengamanan jaringannya.

1.5. Manfaat Penelitian

Hasil penelitian ini diharapkan bermanfaat untuk mengendalikan atau mengontrol keamanan pada jaringan layanan *cloud computing*. Manfaat lain penelitian ini dapat membantu *administrator* jaringan dalam mengantisipasi serangan ke *server*. Penelitian ini dapat diterapkan pada jaringan dengan skala lebih besar.

1.6. Sistematika Penulisan

Penulisan skripsi yang berjudul "Implementasi *Honeypot* Pada *Cloud Computing* Untuk Identifikasi Serangan *Malware*" mempunyai sistematika penulisan sebagai berikut.

BAB I PENDAHULUAN

Bab ini merupakan pendahuluan yang menjelaskan tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menjelaskan landasan-landasan teori yang digunakan sehubungan dengan implementasi *honeypot* untuk mengidentifikasi serangan *malware* pada layanan *cloud computing*.

BAB III METODE PENELITIAN

Bab ini menjelaskan kebutuhan alat dan bahan yang digunakan dalam penelitian dan alur kerja penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas hasil dari pengujian *honeypot* dengan aplikasi *Dionaea* untuk mengindentifikasi serangan *malware* pada layanan *cloud computing*.

BAB V PENUTUP

Bab ini merupakan akhir dari penulisan skipsi berupa kesimpulan dan saran yang diperoleh dari penerapan *honeypot* pada layanan *cloud computing* untuk mengindentifikasi serangan *malware*.