BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Cloud computing merupakan suatu istilah dari sebuah teknologi pemanfaatan internet lebih jauh untuk yang dimana semua proses komputasi, komunikasi, software, data akses dan media penyimpanan diserahkan kepada pihak ke tiga, dan user hanya perlu membayar layanan yang digunakan serta tidak perlu tahu dimana lokasi fisik data-data user tersebut disimpan. Dengan diterapkannya cloud computing, suatu perusahaan/instansi/pengguna dapat menghemat biaya yang dikeluarkan untuk pengembangan aplikasi bisnisnya karena tidak perlu membuang biaya untuk membeli/mengganti sumber daya yang sudah ada, hanya perlu koneksi internet untuk menjalankan aplikasi bisnisnya.

Cloud computing dibagi menjadi dua yaitu, public cloud dan private cloud. Public cloud merupakan layanan cloud yang dijual lewat internet oleh perusahaan, sedangkan private cloud merupakan layanan cloud yang berada pada jaringan LAN dan dengan apabila private cloud semakin berkembang, maka secara tidak langsung dapat memajukan infrastruktur internet Indonesia. Dengan semakin banyak pengguna cloud computing, ada satu hal yang sangat perlu diperhatikan dan tidak bisa diabaikan yaitu masalah kemanan (security issue). Perusahaan maupun user yang menggunakan layanan cloud computing, tentu tidak ingin data-data yang bersifat rahasia dapat diakses oleh pihak yang tidak berhak. Salah satu metoda penanganan dalam hal security adalah menggunakan firewall serta sistem pendeteksi penyusupan atau Intrusion Detection Sistem (IDS) yang diterapkan/ditempatkan sistem keamanan tersebut antara jaringan luar dan jaringan dalam (Private Cloud) yaitu pada PC Router. Ada beberapa versi dari firewall dan IDS yaitu versi berbayar atau berlisensi sampai yang bersifat opensource. Keduanya tentu mempunyai kelebihan dan kekurangan masing-masing.

Pada penelitian sistem keamanan jaringan private cloud ini, digunakan sistem keamanan firewall serta IDS yang bersifat opensource. Harapannya dengan diterapkan firewall dan IDS pada PC Router tersebut, jaringan private cloud menjadi lebih aman dari ancaman dari Network Penetration dan usaha pengumpulan informasi yang mungkin terjadi seperti serangan DOS (Denial Of Service), Port Scanning, dan lain-lain. Sehingga tools pengujian keamanan yang digunakan adalah menggunakan Nmap (Network Mapper) dan Hping3. Kedua tools ini telah menjadi standar de facto dalam pengujian sistem serta banyak digunakan oleh security analyst. Selanjutnya, dengan adanya IDS maka paket-paket yang memiliki ciri-ciri (signature) serangan yang masuk ke PC Router, admin dapat mengetahui serangan tersebut dalam waktu singkat dengan membaca alert message-nya dan melakukan tindakan preventif dari IDS tersebut dengan memblok alamat sumber paket tersebut. Dengan demikian pengguna dapat merasa lebih nyaman untuk menyimpan data pribadinya, serta server dapat lebih aman.

1.2 Maksud dan Tujuan

Dalam penelitian ini dimaksudkan dibuat sistem keamanan berupa firewall untuk mengamankan jaringan Cloud Computing. Dimana pada sistem keamanan tersebut ditambahkan fitur Log Analysis terhadap paket yang di-log oleh firewall karena tidak sesuai dengan rules yang diterapkan di sistem keamanan. Serta ditambahkan pula suatu sistem untuk melakukan tindakan aktif/preventif dalam menanggapi serangan tersebut yaitu salah satunya memblok alamat sumber paket secara otomatis. Dengan adanya fitur-fitur keamanan ini apabila ada suatu usaha pengintaian, pencarian informasi layanan dan serangan DOS terhadap jaringan private cloud yang masuk/melewati sistem keamanan, maka sistem keamanan akan berusaha menganalisis usaha serangan ataupun ancaman apa saja yang dilakukan terhadap jaringan private cloud. Dan apabila usaha tersebut itu melebihi batas toleransi yang ditentukan oleh IDS, maka alamat sumber yang melakukan usaha pengumpulan informasi atau DOS tersebut akan di-blok.

Adapun tujuan akhir yang ingin dicapai dalam penelitian ini adalah dengan diterapkannya firewall dalam jaringan private cloud, maka jaringannya tersebut dapat menjadi lebih aman dan terlindungi dari serangan dan ancaman dari luar

jaringan private cloud yang mungkin terjadi serta meminimalisir kemungkinan terjadinya pencurian data dan lain-lain.

1.3 Batasan Masalah

Penelitian ini memiliki batasan masalah sebagaimana berikut:

1. Sistem kemanan yang dirancang hanya menghalau serangan maupun ancaman yang berasal dari luar jaringan Private Cloud, yaitu Port Scan serta DOS (Denial Of Service) bertipe ICMP Flood.
2. Sistem Operasi untuk PC Router yang digunakan pada penelitian tugas akhir ini adalah Linux Ubuntu 10.04 LTS.
3. Tools keamanan yang digunakan dalam membangun sistem keamanan pada PC Router adalah sebagaimana berikut:
   a. Iptables (Firewall)
   b. Psad (Log Analysis dan IDS)
4. Tools pengujian keamanan yang digunakan dalam adalah sebagai berikut:
   a. Nmap (Network Mapper)
   b. Hping3
5. Ditambahkan fitur log analysis dari psad untuk melakukan analisis terhadap paket yang di-log dan secara opsional digunakan fitur IDS pada psad untuk mendeteksi serangan sesuai dengan ciri-ciri serangan tersebut (signature), dan bila memungkinkan melakukan aksi preventif terhadap serangan tersebut.

1.4 Metoda Penelitian

Dalam melakukan penelitian ini, akan digunakan beberapa tahap dalam menyelesaikan penelitian, diantaranya adalah:

1. Studi Literatur

   Metoda ini digunakan untuk mendapatkan informasi dan pengetahuan dari literatur-literatur yang sudah ada, baik dari buku, jurnal ilmiah, dan internet.
2. Perancangan Sistem

   Perancangan terhadap model sistem keamanan yang akan digunakan dan diimplementasikan. Yang dimana langkah-langkah dalam perancangannya adalah sebagai berikut:

a. Menggunakan dan mengkonfigurasi tools firewall yang digunakan yaitu iptables/netfilters.
b. Membuat policy dan rules yang akan diterapkan pada sistem keamanan.
c. Menambahkan fitur log analysis dari psad dan sistem deteksi penyusupan (IDS) dari psad untuk meningkatkan keamanan sistem jaringan.
d. Uji keamanan terhadap sistem yang telah dirancang dengan tools uji keamanan.

3. Implementasi Sistem

   Untuk mengetahui kinerja dan kehandalan sistem, maka model sistem yang telah dirancang akan diterapkan kepada jaringan private cloud.

4. Pengujian Sistem

   Sistem keamanan yang telah diimplementasi kemudian diuji kehandalannya dengan cara melakukan uji keamanan dari PC yang difungsikan sebagai penyerang (Attacker PC) terhadap Server.

5. Analisis dan Kesimpulan

   Sistem keamanan yang telah diimplementasi serta diuji coba kemudian dari hasil dan data yang didapat, dianalisis serta membuat kesimpulan apakah sistem keamanan yang dirancang dapat membuat jaringan private cloud/ server lebih aman atau tidak.

1.5 Sistematika Penulisan

Sistematika penulisan tugas akhir ini meliputi:

BAB I PENDAHULUAN

Bab ini berisi penjelasan mengenai latar belakang masalah, tujuan dan manfaat, batasan masalah, metodologi penelitian, dan sistematika penulisan.

BAB II DASAR TEORI

Bab ini menguraikan tentang teori-teori yang menunjang dasar-dasar perancangan sistem.

BAB III PERANCANGAN SISTEM

Bab ini menguraikan tentang perancangan sistem yang akan dirancang dalam penelitian tugas akhir ini.

BAB IV PENGUJIAN DAN ANALISA

Bab ini menguraikan hasil pengujian sistem yang telah dirancang, pengambilan data, dan analisa pengujian sistem.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari hasil pengujian, dan saran-saran yang menunjang ke arah pengembangan penelitian yang telah di lakukan dalam penelitian ini.