BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Perkembangan teknologi saat ini memungkinkan pengguna dapat mengakses suatu layanan melalui jaringan internet dengan lebih mudah. Dengan makin pesatnya perkembangan teknologi jaringan, hal ini justru menjadi momok menakutkan dengan munculnya ancaman serangan cyber. Menurut data yang dirilis oleh CrowdStrike pada tahun 2024, serangan cyber cenderung meningkat 60% dari tahun ke tahun. Lini teknologi merupakan salah satu industri paling banyak terjadi serangan sebesar 23% dibandingkan dengan industri lainnya. Jenis serangan yang dilakukan oleh penyerang biasanya menggunakan metode phishing untuk menyamar sebagai pengguna yang sah agar bisa melakukan manipulasi ke akun yang valid, sehingga penyerang dapat mengambil alih suatu komputer target [1].

Agar serangan tidak terjadi secara langsung ke komputer utama, maka perlu adanya lapisan keamanan tambahan pada sistem jaringan. Terdapat berbagai macam mekanisme untuk dapat mengamankan jaringan sembari memfasilitasi layanan internet ke klien, salah satunya adalah menggunakan *bastion server*. *Bastion server* dapat melindungi sistem jaringan dari serangan luar. Representasi dari *bastion server* biasanya berupa komputer berbasis Linux yang dilengkapi berbagi macam konfigurasi keamanan [2].

Selama ini untuk menyediakan dan mengkonfigurasi *bastion server* masih banyak menggunakan cara manual, dimana penerapannya banyak memerlukan campur tangan manusia [3]. Namun, hal ini justru menimbulkan resiko kesalahan akibat dari pekerjaan yang repetitif, baik dari tahap konfigurasi hingga deployment. Terlebih lagi, semakin kompleks konfigurasi yang dilakukan akan menambah beban kerja manusia dan menghabiskan waktu yang tidak sedikit. Perlu adanya suatu platform yang

dapat memonitoring dan mengotomasi sistem agar mempermudah manusia membuat infrastruktur komputer sehingga manusia bisa lebih fokus terhadap aspek bisnis daripada mengurusi pekerjaan operasional yang berulang.

Mengacu pada beberapa penelitian sebelumnya, manajemen konfigurasi seperti *Ansible* kerap kali digunakan untuk mengokestrasi *server* baik yang bersifat bare metal ataupun virtual. Pemanfaatan *Ansible* dinilai cukup membantu proses konfigurasi *server*, apalagi jenis *server* yang membutuhkan banyak pengesetan, contohnya ialah *Bastion server*. Oleh karena itu, penulis terinsipirasi untuk merancang sistem infrastruktur *server* berupa *bastion server* yang dijalankan dalam arsitektur *Demilitarized Zone*. *Ansible* dipilih karena beberapa kelebihan yang dimilikinya jika dibandingkan dengan platform lain, diantarany adalah pengaplikasiannya yang mudah, skalabilitas yang tinggi, fleksibel saat dihubungkan dengan perangkat lain, dan harga layanan yang terjangkau. Nantinya, rancangan sistem akan memanfaatkan *Ansible* untuk menyediakan dan mengokestrasi beberapa *bastion server* sekaligus. Diharapkan perancangan sistem akan mempermudah proses operasional infrastuktur .

Berdasarkan latar belakang di atas, penulis bermaksud mengangkat topik ini menjadi tugas akhir dengan judul "Penerapan Ansible Untuk Mengokestrasi Bastion server dengan Sistem Demilitarized Zone".

1.2. Perumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka dapat dibuat suatu rumusan masalah sebagai berikut:

1. Pemanfaatan *bastion server* untuk mitigasi serangan berlanjut
2. Efisiensi waktu untuk mengkonfigurasi sejumlah *bastion server* sekaligus
3. Perancangan sistem infrastruktur dengan usaha yang minimal dalam mengkonfigurasi beberapa *bastion server*

4. Pencegahan kesalahan konfigurasi *bastion server* dengan menerapkan integrasi melalui satu platform yang meliputi monitoring, manajemen, dan penyebaran

1.3. Pertanyaan Penelitian

Berdasarkan latar belakang diatas, maka dapat diambil beberapa pertanyaan seperti berikut:

1. Bagaimana cara merancang *bastion server* untuk mitigasi serangan berlanjut?
2. Bagaimana cara memanfaatkan manajemen konfigurasi seperti *Ansible* untuk menyediakan dan mengokestrasi sistem *bastion server*?
3. Apa hasil laporan keamanan dari infrastrutkur yang telah dibuat?

1.4. Batasan Masalah

Berdasarkan latar belakang diatas, perlu adanya pembatasan agar penelitian bisa lebih focus dan terarah, berikut adalah batasan masalahnya :

1. Pengujian *Ansible* dilakukan di *Linux RHEL* versi 9.0
2. Implementasi manajemen konfigurasi menggunakan *Ansible* versi 3.0.0
3. Pengujian sistem menggunakan metode *Black Box*

1.5. Tujuan Penelitian

Berdasarkan perumusan masalah di atas, maka tujuan yang akan dicapai dalam penelitian ini adalah sebagai berikut :

1. Merancang infrastrukur *bastion server* dengan sedikit konfigurasi menggunakan *Ansible*
2. Penerapan *bastion server* untuk menghalau serangan

1.6. Manfaat Penelitian

Adapun manfaat dari penulisan skripsi, dapat diuraikan sebagai berikut:

1. Manfaat Praktis :
   a. Bagi Peneliti

      Sebagai syarat untuk meraih gelar sarjana informatika di Fakultas Informatika Universitas Telkom Purwokerto

   b. Bagi Kampus

      Hasil penelitian dapat dijadikan referensi dalam pengembangan ilmu pengetahuan teknologi terutama pemanfaatan *platform* otomasi dalam menunjang kebutuhan infrastrutktur

   c. Bagi Konsumen

      Hasil penelitian dapat memepermudah manusia dalam mengelola *server* terutama *bastion server* secara otomatis.

2. Manfaat Teoritis :

   Hasil penelitian ini dharapkan dapat menjadi gambaran untuk dikembangkan oleh peneliti lain dalam memecahkan masalah serupa maupun sector lainnya serta mengetahui perbedaan metode okestrasi yang berbeda.