BAB 1. PENDAHULUAN

1.1 Latar Belakang

Menurut kamus besar dan pakar–pakar teknologi, jaringan komputer adalah sebuah sistem operasi yang terdiri atas sejumlah komputer dan perangkat jaringan lainnya yang berkerja bersama-sama untuk mencapai suatu tujuan yang sama atau suatu jaringan kerja yang terdiri dari titik-titik (*Nodes*) yang terhubung satu sama lain. Masing-masing *nodes* berfungsi sebagai stasiun kerja dan dua buah komputer yang masing-masing memiliki sebuah kartu jaringan, kemudian dihubungkan melalui kabel maupun nirkabel sebagai medium transmisi data dan terdapat perangkat lunak sistem operasi jaringan akan membentuk sebuah jaringan komputer yang sederhana yang biasa disebut local area network. Setiap jaringan komputer yang terhubung tidak ada jaminan sebuah keamanan. Maka dari itu dalam Jaringan komputer terdapat sistem yang dinamakan Firewall. Firewall adalah sebuah sistem atau perangkat yang memberi otorisasi pada lalu lintas jaringan komputer yang dianggapnya aman dan melakukan pencegahan terhadap jaringan yang di anggap tidak aman. Terdapat banyak ancaman pada serangan jaringan komputer, salah satunya adalah brute force. Brute force adalah suatu serangan pada server, jaringan, dan host dengan cara mencoba kemungkinan kombinasi password yang ada pada *wordlist* (Kamus Password). Maka dari itu *port knocking* berperan penting dalam mengatasi masalah ini. *Port knocking* adalah suatu sistem keamanan yang bertujuan untuk membuka dan menutup port tertentu dengan menggunakan firewall pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi bisa berupa protocol TCP, UDP, dan ICMP.

Salah satu laboratorium di Gedung Teknologi Informasi terdapat suatu koneksi jaringan yang sangat padat. Hampir setiap hari para mahasiswa Teknologi Informasi menggunakan koneksi tersebut. Sehingga sistem keamanan jaringan pada

laboratorium sangat rawan sekali untuk diretas oleh pihak-pihak yang tidak bertanggung jawab. Dengan adanya ancaman-acaman tersebut, maka sistem keamanan jaringan pada Laboratoriun AJK di Gedung Teknologi Informasi Politeknik Negeri Jember dapat dicegah secepat mungkin. Karena jika tidak dicegah, para peretas dapat mengacaukan konfigurasi router tersebut lewat port-port yang sedang terbuka. Sehingga koneksi jaringan menjadi kacau dan data-data yang terdapat pada router dapat diketahui oleh orang lain. Sebelum kejadian itu terjadi, maka penulis dapat mengatasinya dengan menerapkan metode *Port Knocking* dan *De-Militarized Zone*. Dengan hal ini, maka sistem keamanan jaringan yang ada pada Lab. AJK bisa berjalan dengan lancar dan lebih aman.

1.2 Rumusan Masalah

Dari latar belakang di atas, maka dapat di simpulkan berbagai permasalahan yang ada di jaringan komputer, diantaranya adalah :

1. Bagaiman cara memperkuat kinerja firewall agar sistem keamanan dan data pada Lab. AJK menjadi lebih aman.
2. Bagaimana mengatasi sistem keamanan jaringan agar terbebas dari serangan hacking port.

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas maka tujuan dari penelitian yaitu :

1. Memaksimalkan keamanan router untuk blocking port pada jaringan menggunakan router mikrotik.
2. Meminimalisir serangan brute force dari luar yang bertujuan untuk merusak konfigurasi pada router.

1.4 Manfaat penelitian

Adapun manfaat yang diharapkan dari penelitian ini adalah :

1. Meningkatkan keamanan router untuk blocking port dan pengalihan IP server demi kenyamanan dan keamanan pengguna.
2. Dengan adanya blocking port dan pengalihan IP server maka jaringan komputer dapat berkerja dengan optimal, sehingga membuat transfer data menjadi aman dan lancar.