BAB I

PENDAHULUAN

1.1. Latar Belakang

Keamanan jaringan merupakan salah satu hal terpenting dalam implementasi jaringan komputer. Tidak sedikit jaringan komputer yang mengalami masalah yang disebabkan oleh kelalaian pengelola jaringan dalam membangun sebuah jaringan komputer. Dikarenakan kelalaian tersebut sehingga dapat membuka peluang bagi para orang-orang yang tidak bertanggung jawab untuk meretas dan merusak jaringan yang dibangun tersebut.

Dengan pesatnya perkembangan teknologi internet saat ini, tidak dapat dipungkiri akan berdampak pada meningkatnya *cyber crime*. Serangan-serangan tersebut sering dilakukan pada suatu port yang dalam keadaan terbuka, sehingga nantinya akan membuat orang–orang yang tidak mempunyai hak akses maupun yang tidak berkepentingan dapat dengan mudah mengendalikan port–port yang telah dimasuki.

Ketika diperlukan untuk menjalin komunikasi dengan apa yang ada di dalam jaringan komputer, *firewall* tidak mengizinkannya karena mungkin memang berada pada area yang tidak diizinkan. Padahal komunikasi yang ingin dilakukan sangatlah penting untuk kelancaran kerja. Misalnya, kita terkoneksi dengan Internet dan butuh masuk ke dalam web server melalui SSH (*Secure Shell)* untuk memperbaiki konfigurasinya, sementara port SSH pada server tersebut dilarang untuk diakses dari Internet.

Pada gedung jurusan Teknik Komputer Politeknik Negeri Sriwijaya, terdapat beberapa router mikrotik, ada kemungkinan router-router tersebut dapat diakses orang-orang yang tidak bertanggungjawab. Maka dari itu dibutuhkan suatu sistem keamanan yang tidak hanya aman dari serangan-serangan tersebut tetapi juga nyaman bagi administrator yang tetap ingin memiliki koneksi pribadi ke dalamnya secara kontinyu

dan dapat dilakukan dari mana saja. Metode pengamanan yang dapat dilakukan didalam sistem pengamanan jaringan komputer salah satunya adalah metode Port knocking. Metode ini dapat diterapkan pada beberapa *port* komunikasi yang biasanya merupakan *port* yang ada dalam protokol TCP (*Transmission Control Protocol*) atau UDP (*User Datagram Protocol)* yang merupakan anggota dari *Transportation layer* pada standar OSI (*Open System Interconnection)*.

Dengan mempertimbangkan semua hal di atas, penulis membuat laporan akhir yang berjudul "**Sistem Keamanan Jaringan Komputer Pada Router Dengan Metode *Port Knocking* Pada Jurusan Teknik Komputer Politeknik Negeri Sriwijaya**".

1.2. Rumusan Masalah

Berdasarkan latar belakang diatas adapun rumusan masalah yang didapat yaitu Bagaimana cara mengkonfigurasi sistem keamanan dengan metode *Port Knocking* pada Router Jaringan Komputer di Jurusan Teknik Komputer.

1.3. Batasan Masalah

Agar penulisan Laporan Akhir ini lebih terarah dan tidak menyimpang dari permasalahan yang ada, maka penulis membatasi pokok permasalahan hanya pada hal-hal seperti :

1. Menggunakan metode *Port Knocking* untuk mengamankan router dari serangan-serangan *cyber*.
2. Membuat *Filter rule* baru pada winbox guna menerapkan metode *Port knocking* pada router.

1.4. Tujuan

Adapun Tujuan dari pembuatan laporan akhir ini adalah sebagai berikut :

1. Meminimalisir terjadinya penyalahgunaan jaringan oleh orang-orang yang tidak bertanggung jawab.
2. Menutup seluruh port pada router, dan hanya memberikan akses kepada pengguna yang sudah melewati *filter rule* yang telah dibuat.

1.5. Manfaat

Adapun manfaat dari pembuatan laporan akhir ini adalah:

1. Dapat meminimalisir serangan *cyber* yang ditujukan pada router.
2. Pengguna / administrator dapat menggunakan router dengan aman dan nyaman.