BAB I

PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer saat ini mengalami perkembangan yang sangat pesat, dalam kemajuan sistem jaringan komputer ini juga tidak hanya membawa dampak positif saja, melainkan juga dampak negatif. Kejahatan-kejahatan baru kian muncul, yang tadinya menggunakan teknik yang biasa, sekarang menggunakan teknik yang lebih *modern*.

Sebagai contoh pada jaringan Internet terdapat dua sisi yang saling bertentangan dalam hal akses pencarian informasi. Di satu sisi, banyak usaha-usaha dilakukan untuk menjamin keamanan suatu sistem dalam hal akses pencarian informasi, di sisi lain ada pihak-pihak dengan maksud tertentu yang berusaha untuk melakukan eksploitasi sistem keamanan tersebut. Eksploitasi keamanan adalah berupa serangan terhadap keamanan sistem informasi.

Berbagai bentuk serangan atau ancaman seperti *Virus, Trojan, Worm, DDoS, hacker, cracker*, dan sebagainya yang dapat membahayakan sistem keamanan data komputer dan dapat menurunkan performa jaringan, apabila ancaman-ancaman ini ”menyerang”. Biasanya bentuk ancaman ini dapat menyerang masuk ke sistem komputer melalui *port-port* terbuka yang tidak digunakan dalam sistem jaringan .

Oleh karena itu untuk memberikan proteksi terhadap bermacam bentuk serangan yang kemungkinan terjadi dalam jaringan komputer dibutuhkan suatu mode keamanan seperti *firewall*. *Firewall* adalah sistem keamanan yang melindungi komputer dari berbagai ancaman di jaringan internet. *Firewall* ini bekerja sebagai sekat atau tembok yang membatasi komputer dari jaringan internet.

Berdasarkan penelitian yang telah dilakukan sebelumnya , Menurut Sumardi dan Ramadhian Agus Triyono (2013:16) menjelaskan bahwa Di dalam sistem komputer terdapat *firewall* yang berfungsi untuk mencegah gangguan tersebut, namun dengan kemampuan yang terbatas. Oleh karena itu dibutuhkan

perangkat tambahan yang dapat membantu tugas *firewall*. Salah satu perangkat yang memungkinkan melaksanakan tugas tersebut adalah *router*. Dengan penambahan *router* diharapkan sistem keamanan dan data komputer yang ada akan lebih kuat.

Sejauh ini sistem keamanan jaringan komputer di laboratorium jurusan teknik komputer masih belum menggunakan *router (firewall)* yang berfungsi untuk memblokir port-port yang tidak digunakan sehingga risiko masuknya *malware* dan serangan dari luar kemungkinannya masih sangat besar. Dengan adanya *firewall* yang akan memblokir port-port terbuka yang tidak digunakan tersebut, maka jaringan komputer lokal akan lebih terlindungi. Dalam pengimplementasian *firewall* ini, dikarenakan terbatasnya ruang pada laboratorium jurusan teknik komputer akan terasa lebih efektif apabila menggunakan *routerboard* dibandingkan *PC router* sebagai media *firewall* nya. Dan sistem operasi *(software)* yang digunakan adalah sistem operasi mikrotik. Karena mikrotik merupakan salah satu sistem operasi yang dapat digunakan sebagai *router* jaringan yang handal, dan mencakup berbagai fitur lengkap untuk jaringan komputer.

Dengan demikian, penulis bermaksud menerapkan sistem yang berjudul **"Implementasi Sistem Keamanan Jaringan Komputer Menggunakan *Blocking Port* Pada Laboratorium Jurusan Teknik Komputer".**

1.2 Perumusan Masalah

Berdasarkan latar belakang diatas, perumusan masalah yang ada, yaitu :

1. Bagaimana cara membangun *rule firewall* dan memperkuat kinerja *firewall* untuk memblokir *port-port* yang tidak digunakan melalui *router* mikrotik pada laboratorium jurusan teknik ?.
2. Bagaimana mengatasi celah keamanan dan meminimalisir kemungkinkan masuknya *malware* dan serangan dari luar yang bertujuan memperlambat jaringan lokal melalui *port-port* yang terbuka ?.

1.3 Batasan Masalah

Adapun batasan masalah agar pembahasan pokok masaalah tidak menyimpang dan melebar, maka penulis hanya akan membahas :

1. Konfigurasi untuk sistem *router* yang terdiri dari setting *IP Address*, *default gateway*, DNS (*Domain Name Server*) dan NAT (*Network Address Translation*).
2. Memblokir *port-port* tertentu yang tidak digunakan dalam jaringan tempat masuknya *malware* dan serangan yang bertujuan memperlambat jaringan dari internet.
3. Dalam pemblokiran *port*, hanya *port* tertentu yang sudah ketahui atau didefinisikan (*well-known port*) oleh *Internet Assigned Number Authority* (IANA)

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Adapun tujuan dari perancangan sistem ini adalah :

1. Memaksimalkan kinerja atau kemampuan perangkat *routerboard* untuk *blocking port* pada jaringan lokal laboratorium jurusan teknik komputer
2. Meminimalkan resiko masuknya *malware* dan serangan dari luar yang dapat memperlambat jaringan melalui internet ke jaringan lokal laboratorium jurusan teknik komputer.

1.4.2 Manfaat

Manfaat dibuatnya Sistem Keamanan ini adalah :

1. Dengan meningkatnya kinerja ataupun kemampuan perangkat *routerboard* untuk *blocking port* diharapkan mahasiswa merasakan kenyamanan pada saat melakukan kegiatan praktikum.
2. Dengan tidak adanya penyebaran *malware* dan serangan dari luar diharapkan jaringan komputer menjadi aman