BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan jaringan merupakan salah satu aspek yang wajib terdapat pada suatu jaringan komputer. Dimana ketika saling berbagi informasi melalui internet, maka suatu keamanan jaringan sangat dibutuhkan. Terutama pada sebuah lembaga baik yang berupa perusahaan, kantor pemerintah, perguruan tinggi maupun individual. Kebutuhan manusia yang tidak lepas dari komunikasi dan informasi, hal itu menjadikan keamanan jaringan ini sangat dan harus ada dalam sebuah system jaringan tersebut sehingga dapat diandalkan untuk dapat memenuhi kebutuhan kehidpan bermasyarakat [7].

Dengan adanya suatu keamanan jaringan, akan membuat Lembaga tersebut terhindar dari *cybercrime*. Dalam Kamus Besar Bahasa Indonesia (KBBI), *cybercrime* diartikan sebagai kejahatan siber ialah tindak pidana yang bersangkutpaut dengan kehidupan dunia maya, sistem komputer, sistem informasi atau internet [10]. *Cybercrime* dapat terjadi jika tingkat keamanan pada suatu jaringan tersebut sangat rendah, sehingga data pengguna tidak tersimpan dengan aman. *Cybercrime* dapat kita hindari dengan cara membuat sistem keamanan yang dapat mengamankan server yang terhubung dengan internet. Salah satu cara untuk mencegah *cybercrime* ini adalah yaitu menggunakan metode *De-Militarized Zone* (*DMZ*) [5].

De-Militarized Zone (DMZ) adalah satu antar muka yang diletakan di suatu tempat antara *local network* dan *public network* yang mampu memberi isolasi nyata ditengah kedua jaringan, didukung oleh sebuah aturan konektivitas di *firewall. De-Militarized Zone* (DMZ) merupakan suatu pengaman yang sangat dibutuhkan karena dia hanya memberi izin akses internet menuju server yang telah dipisahkankan di *De-Militarized Zone (DMZ)* terlebih dahulu, dan tidak langsung memasuki jaringan internal. *De-Militarized Zone (DMZ)* memiliki tiga jenis konfigurasi yaitu *single firewall, dual firewall, dan screened-subnet*. Untuk mengkoneksikan antara jaringan internal dan eksternal seperti jaringan internet, maka harus mengatur *traffic*

packet menggunakan perangkat *firewall* serta diperkuat dengan *security policy*.

Keamanan jaringan telah diatur dalam Peraturan Menteri Komunikasi dan Informatika Nomor: 16/PER/M.KOMINFO/10/2010 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. Dengan adanya Undang-undang tersebut menjadikan seluruh lembaga pemerintahan atau instansi memiliki suatu keamanan jaringan yang bermacam-macam salah satunya *De-Miltiarized Zone* (DMZ) [5].

Penerapan sistem keamanan jaringan dengan menggunakan teknik *De-Miltiarized Zone* (DMZ) diusulkan sebagai salah satu solusi yang dapat digunakan dalam mengamankan jaringan dari suatu area yang kemungkinan ada serangan *hacker* (*hack attack*) dari pihak luar jaringan. *De-Miltiarized Zone* (DMZ) diterapkan karena dianggap mampu mendeteksi serta dapat menghindari serangan berbahaya pada jaringan, dan juga *De-Miltiarized Zone* (DMZ) berfungsi sebagai perubahan konfigurasi terhadap jarinagn lainnya supaya tetap aman dari serangan *hacker* [5].

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan maka terdapat beberapa rumusan masalah yang muncul sebagai dasar penelitian yaitu :

1. Cara kerja *De-Militarized Zone (DMZ)*
2. Kinerja sistem keamanan jaringan dengan teknik *De-Militarized Zone (DMZ)*

1.3 Pertanyaan Penelitian

1. Bagaimana cara kerja *De-Militarized Zone (DMZ)* dalam mengamankan suatu jaringan?
2. Apakah system keamanan jaringan dengan teknik *De-Militarized Zone (DMZ)* yang diterapkan dapat berfungsi dengan baik?

1.4 Batasan Masalah

Berikut dua pertimbangan batasan masalah yang diterapkan pada penelitian:

1. Penulis akan membahas simulasi sistem keamanan jaringan komputer dengan teknik *De-Militarized Zone (DMZ)*.
2. Penulis hanya membuat simulasi keamanan jaringan dengan topologi *De-Militarized Zone (DMZ)*.

1.5 Tujuan Penelitian

Adapun tujuan pada penelitian ini yaitu :

1. Membuat simulasi teknik *De-Militarized Zone (DMZ)* untuk pengamanan jaringan komputer dengan menggunakan GNS3.
2. Mengetahui performa keamanan jaringan dengan menggunakan teknik *De-Militarized Zone (DMZ).*

1.6 Manfaat Penelitian

Manfaat dari penelitian ini diharapkan bermanfaat bagi :

1. Bagi Penulis.

   Sebagai sarana untuk menerapkan pengetahuan yang diperoleh selama masa studi dan sebagai salah satu persyaratan untuk lulus dari program studi S1 Informatika di Institut Teknologi Telkom Purwokerto.
2. Bagi Pengguna / Masyarakat.

   Masyarakat bisa mengetahui performa dari teknik *De-Militarized Zone* dalam mengamankan suatu jaringan komputer.
3. Bagi Institut Teknologi Telkom Purwokerto.

   Hasil dari penelitian ini diharapkan bisa digunakan sebagai rujukan untuk penelitian selanjutnya dan menyumbang pengembangan ilmu pengetahuan untuk Institut Teknologi Telkom Purwokerto.