BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi di bidang informasi sudah sangat berkembang sedemikian pesat, dapat terlihat dari maraknya pemakaian internet di segala bidang baik pribadi ataupun perkantoran. Sistem jaringan yang terbuka memungkinkan terjadinya penyalahgunaan atau kejahatan *cyber*.

Terbukti pada dewasa ini penyalahgunaan atau kejahatan *cyber* semakin marak terjadi. Berdasarkan laporan dari perusahaan keamanan *cyber* Kapersky merilis laporan statistik serangan *cyber* terbaru. Dalam laporan tersebut, Kapersky menjelaskan statistik serangan DOS pada kuartal kedua tahun 2019 tipe serangan DOS yaitu *SYN Flooding* masih mendominasi dengan presentase 82,43%. Selanjutnya disusul tipe serangan UDP *Flood* dengan presentase 10,94%, kemudian posisi ketiga tipe serangan TCP *Request* dengan presentase 3,26% disusul dengan HTTP *traffic* 2,77% dan terakhir ICMP *Flooding* 0,59% [1]. Maka dari itu dalam penelitian ini penulis mengangkat tema berupa kemanan konfigurasi jaringan dari suatu serangan kejahatan *cyber* yang sedang marak terjadi yaitu *SYN Flood*.

Secara umum sistem informasi yang terpusat sangat rawan terhadap berbagai macam serangan seperti *SYN Flood* dan lain sebagainya. Seorang penyerang (*attacker*) akan menyerang sistem jaringan dengan maksud mengalahkan layanan keamanan pada fasilitas jaringan tersebut. Dengan mempertimbangkan fakta bahwa jaringan publik pada awalnya dirancang untuk keterbukaan tanpa mempertimbangkan keamanan, tentunya hal tersebut diikuti pula dengan meningkatnya serangan *cyber* dari tahun ketahun [2].

Serangan *SYN Flood* akan membanjiri server dengan *request* palsu secara bertubi-tubi, mengeksploitasi dan menghabiskan sumber daya jaringan. Pada dasarnya ketika sebuah komputer yang terhubung ke pada suatu *server* maka akan terjadi yang disebut koneksi TCP ke *server*. Dimana *client* mengirim *SYNchronize* ke *server* dan *server* akan mengenali *acknowledge* (ACK) *request* ini dengan mengirim balik SYN-ACK ke *client* dan *client* mengirim ACK maka koneksi akan

terbentuk. Proses hubungan ini juga dikenal dengan sebutan TCP *Three Way Handshake*. Namun pada kasus *SYN Flood* kode yang seharusnya dikirim kembali oleh *client* pada fase terakhir, tidak dikirim kembali justru komputer membuat *request* baru kesemua *port* yang ada pada *server*. Akibatnya koneksi masih terbuka dan tidak bisa ditutup oleh *server* hal ini akan terjadi secara terus-menerus akan mengakibatkan *server* menjadi sangat sibuk [2].

Seiring dengan perkembangan teknologi saat ini telah ditemukan cara untuk menangkal dari serangan *SYN Flood* yang mengacu pada RFC (*Request For Comment*) publikasi nomor 4987 yang salah satu diantaranya yaitu memasang dan mengoptimalkan perangkat *firewall* dan *proxy* [3]. *Firewall* adalah sistem keamanan jaringan komputer yang melindungi perangkat dari *virus, malware, spam, link* dan jenis serangan yang tidak dikenal. *Firewall* adalah perangkat lunak yang bisa mencegah akses data yang dianggap ilegal atau tidak sah dari jaringan[4].

Adapun dalam penelitian ini penulis mengambil beberapa referensi terkait penelitian terdahulu antara lain penelitian yang dilakukan oleh Mhd.Fakhmi dan Lipantri Mashur Gultom dari Teknik Informatika Politeknik Negeri Bengkalis pada tahun 2021 dalam artikel yang berjudul "Peningkatan Keamanan *Router* Mikrotik Terhadap Serangan *SYN Flood* Dengan Menggunakan *Firewall Raw* (Studi Kasus : Sekolah Menengah Kejuruan Negeri 3 Bengkalis)"[5]. Penelitian selanjutnya yaitu yang dilakukan oleh Sahren pada tahun 2021 dalam artikel yang berjudul "Implementasi Teknologi *Firewall* Sebagai Keamanan *Server* Dari *SYN Flood Attack*"[2]. Penelitian selanjutnya yaitu yang dilakukan oleh Mahasi Epi Rahmat Putra Gulo, Devri Suherdi, Syarifah Fadillah Rezky pada tahun 2021 dalam artikel yang berjudul "Pemanfaatan *Firewall* Pada Jaringan Mengunankan Mikrotik RB951Ui – 2HnD"[6]. Penelitian selanjutnya yaitu yang dilakukan oleh Budi Jaya, Yuhandri Yunus dan Sumijan dari Universitas Putra Indonesia YPTK Padang pada tahun 2020 dalam artikel yang berjudul "Peningkatan Keamanan *Router* Mikrotik Terhadap Serangan *Denial Of Service* (Dos)"[7]. Penelitian selanjutnya yaitu yang dilakukan oleh Doni Aprilianto, Triyana Fadila dan Much Aziz Muslim pada tahun 2017 dalam artikel yang berjudul "Sistem Pencegahan UDP DNS *Flood* Dengan *Filter Firewall* Pada *Router* Mikrotik"[8].

Berdasarkan hal diatas maka penulis mengangkat topik penelitian berupa Implementasi Keamanan Jaringan Terhadap Serangan *SYN Flood* Dengan Menggunakan *Firewall Raw* Berbasis *Router*board Mikrotik dengan menggunakan metode penelitian PPDIOO (*Prepare Plan Design Implement Operate Optimize*).

1.2 Rumusan Masalah

Adapun rumusan masalah dalam penelitian ini adalah Bagaimana mengimplementasikan keamanan jaringan terhadap serangan *SYN Flood* yang terjadi dengan menggunakan *firewall raw* berbasis *routerboard* mikrotik?

1.3 Batasan Masalah

Agar penelitian ini dapat mencapai sasaran dan tujuan yang diharapkan, maka batasan masalah yang penulis angkat adalah sebagai berikut :

1. Penulis hanya mengimplementasikan cara meningkatkan keamanan jaringan dari serangan *SYN Flood* dengan menggunakan *firewall raw* yang berbasis *routerborad* mikrotik.
2. Dalam pengujian serangan *SYN Flood* penulis menggunakan virtual box dengan OS Kali-Linux.
3. Klasifikasi *router* yang digunakan adalah *Routerboard* Mikrotik *router wireless* RB-931-2Nd (Hap-Mini) dengan sistem operasi RouterOS dan dikonfigurasi menggunkaan Winbox versi 3.36.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan

Tujuan dari penelitian ini berupa :

1. Agar pembaca dapat memahami dan mengerti pentingnya keamanan pada suatu jaringan komputer.
2. Agar pembaca dapat memahami dan mengimplementasi teknik keamanan jaringan dari serangan *SYN Flood* yang terjadi dengan menerapkan *firewall raw* berbasis mikrotik.

3. Agar jaringan komputer terhindar dari serangan *SYN Flood* yang terjadi dengan menerapkan *firewall raw* berbasis *routerboard* mikrotik.

1.4.2 Manfaat

Beberapa manfaat penelitian ini berupa :

1. Dapat memahami dan mengerti pentingnya keamanan pada suatu jaringan komputer.
2. Dapat memahami serta mengimplementasi teknik keamanan jaringan dari serangan *SYN Flood* yang terjadi dengan menerapkan *firewall raw* berbasis mikrotik.
3. Dapat meminimalisir terjadinya serangan pada komputer *server* berupa sistem jaringan komputer yang dimiliki bisa menangkal kejahatan *cyber* berupa *SYN Flood* dengan menerapkan *firewall raw* berbasis *routerboard* mikrotik.

1.5 Sistematika Penulisan

Untuk memudahkan penulis dalam menulis laporan skripsi ini, maka sistematika penulisan yang digunakan dalam penelitian skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah, dan sistematika penulisan dalam penelitian yang dilakukan.

BAB II LANDASAN TEORI

Bab ini berisi tentang teori dan referensi terkait jaringan komputer, kemanan jaringan, *SYN slood attack*, *firewall*, *router*, mikrotik, OSI, NAT, koneksi TCP serta tinjauan / kajian penelitian terdahulu yang berhubungan dengan penelitian serta landasan teori yang berkaitan dengan masalah dalam penelitian yang dilakukan.

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang jenis metode penelitian yang dilakukan, sumber data yang digunakan, teknik pengumpulan data, dan alat bantu dalam menganalisa masalah yang diteliti.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi tentang pembahasan dalam penyelesaian masalah baik meliputi langkah – langkah dalam penelitian, tahapan perancangan dan konfigurasi, tahap pengujian dan implementasi dan tahap analisa hasil penelitian.

BAB V PENUTUP

Bab ini berisi tentang kesimpulan dan saran dari hasil kegiatan penelitian yang telah dilakukan.