BAB I

PENDAHULUAN

1.1 Latar Belakang

Serangan-serangan terhadap jaringan sangat sering terjadi. Pada saat ini serangan luar yang diluncurkan oleh penyerang semakin banyak dan bervariasi. Salah satu contoh serangan terhadap jaringan adalah serangan *brute force.* Serangan *brute force* adalah salah satu serangan yang terjadi pada jaringan komputer. Serangan ini bertujuan untuk mendapatkan akses *server* dengan mencoba banyak kombinasi *password*.

Ketika membangun sebuah jaringan, tentu dibutuhkan keamanan agar jaringan tidak mudah dibobol dan dimasuki oleh orang-orang yang tidak bertanggung jawab. Salah satu contoh serangan yang membutuhkan keamanan pada *server* jaringan adalah *brute force*. Serangan *brute force* merupakan ancaman dari penyerang yang mencoba untuk *login* dengan menggunakan *protocol* SSH dan telnet untuk mengetahui *password login*. Penyelesaian dalam menebak *password* menggunakan algoritma *Brute force* dapat dengan mudah mencari *password* dengan mengkombinasikan karakter dan panjang *password.* (Arifwidodo et al., 2021)

Sistem keamanan jaringan yang baik merupakan hal yang sangat penting untuk menjaga akses data-data penting pengguna serta menjamin kenyamanan dalam penyimpanan data bagi penggunaannya. Hal ini harus di perhatikan karena keamanan jaringan sangat penting untuk melindungi data dari berbagai macam serangan dan usaha-usaha penyusupan atau pemindaian data oleh pihak yang tidak bertanggung jawab.

Kerugian yang dialami apabila terkena serangan *brute force* diantaranya peretas bisa saja menyamar sebagai pemilik akun asli dan mengirim *link Phising* atau menyebarkan konten palsu dan peretas bisa mengubah situs website dengan tujuan untuk merusak reputasi suatu perusahaan atau organisasi. Tentu saja ini sangat merugikan apabila perusahaan atau organisasi tersebut terkena serangan *brute force.* (Silvia, 2021)

Serangan *brute force* sering menyerang pada pada *port* ssh dan *port* telnet dikarena kan port SSH merupakan sebuah protokol jaringan yang membantu pengguna terutama administrator sistem untuk dapat mengakses perangkat secara aman meski melalui jaringan yang tidak aman. Terlebih lagi, SSH dapat digunakan untuk mengakses perangkat dari jarak yang sangat jauh. Semantara Port Telnet adalah protokol tingkat 3 dimana fungsi yang ditawarkan adalah membuat sebuah terminal atau sebuah proses yang terhubung langsung dengan sistem yang dituju sehingga dapat secara langsung memanipulasi sistem yang dituju.(An & Falahuddin, n.d.)

Mikrotik Routerboard merupakan salah satu jenis *router* yang memiliki fitur yang lengkap untuk mendukung keamanan jaringan seperti *firewall. Firewall* akan menyaring data yang diterima dan melacak koneksi yang dibuat untuk menentukan data apakah koneksi diizinkan atau ditolak. Meskipun *firewal* tidak dapat mencegah serangan secara keseluruhan setidaknya *firewall* dapat membantu membuat data menjadi lebih aman dari pada tidak ada *firewall* sama sekali.

Sekolah Menengah Kejuruan Negeri 1 Merbau merupakan salah satu lembaga pendidikan di Indonesia yang berada di kepulauan meranti. Selama ini sistem keamanan yang diterapkan di SMKN 1 Merbau hanya menggunakan *gateway* dan *routing* karena menganggap tidak akan ada penyerangan yang demikian. Hal tersebut tidaklah benar, serangan pada jaringan ini sangat mungkin terjadi apabila tidak ada keamanan Oleh karena itu Penelitian ini bertujuan untuk memberikan pemahaman saat terjadi serangan terhadap perangkat *router mikrotik* terutama terhadap serangan *brute force* dengan melakukan peningkatan keamanan jaringan menggunakan fitur pada *router mikrotik* yaitu *firewall.*

1.2 Rumusan Masalah

Dari uraian Latar Belakang diatas, penulis dapat menyimpulkan beberapa rumusan masalah yaitu:

1. Bagaimana membangun keamanan *Local area network* (LAN) di SMK N 1 Merbau.

2. Bagaimana melakukan pengujian pada *router mikrotik* terhadap serangan *Brute force*
3. Bagaimana mengatasi serangan *Brute force* dengan menggunakan *firewall*

1.3 Batasan Masalah

Untuk menghindari adanya penyimpangan maupun pelebaran pokok masalah dalam penyusunan penelitian ini maka di buat batasan masalah yaitu :

1. Alat yang digunakan yaitu *Mikrotik Router*
2. Metode pengamanan menggunakan *firewall filter rules* pada *mikrotik*
3. Penyerangan dilakukan menggunakan sistem operasi *Kali Linux.*
4. Ruang lingkup jaringan yang diuji yaitu *local area network* pada SMK N 1 Merbau.

1.4 Tujuan dan Manfaat

Adapun tujuan dan manfaat dari Tugas Akhir ini adalah :

1.4.1 Tujuan

Berdasarkan rumusan masalah yang telah diuraikan diatas, maka tujuan dari penelitian ini adalah:

1. Membangun sistem keamanan jaringan menggunakan *Router MikroTik*.
2. Melakukan penyerangan menggunakan metode *Brute Force Attack* terhadap *router*.
3. Melakukan peningkatan keamanan jaringan menggunakan *Firewall Filter rules* pada *RouterBoard MikroTik*.

1.4.2 Manfaat

Manfaat dari penelitian ini adalah:

1. Dapat memahami cara melakukan pengamanan pada *RouterBoard MikroTik.*
2. Mendapatkan peningkatan keamanan jaringan pada *RouterBoard MikroTik*

1.5 Metode Penyelesaian Masalah

Metode penyelesaian yang dilakukan peneliti yaitu dengan melakukan analisa pada *server* untuk melihat keamanan yang sudah ada pada *server* tersebut sebelum dilakukan penyerangan serta melakukan pengamanan tingkat lanjut kepada server setelah dilakukan penyerangan serta mencari artikel yang berkenaan dengan *Brute Force, firewall*, dan *Mikrotik*.