BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

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

Sebuah jaringan *server* akan dibuat pada Jurusan Teknik Komputer. Ketika membangun sebuah *server* yang baru, tentu dibutuhkan keamanan agar *server* tidak mudah dibobol dan dimasuki oleh orang – orang yang tidak bertanggung jawab. Salah satu contoh serangan yang membutuhkan kemanan pada *server* jaringan adalah *brute force*. Serangan *brute force* adalah salah satu serangan yang berbahaya karena serangan tersebut bertujuan untuk membobol *username* dan *password* pada suatu *server* melalui router.

Pada penelitian sebelumnya yang berjudul "*Brute force Attack Detection And Prevention on a Network Using Wireshark Analysis"* yang dibuat oleh Mustapha Adamu Mohammed, Ashigbi Franlin Degadzo, Botchey Francis Effrim dan Kwame Anim Appiah pada tahun 2017, menjelaskan bahwa mereka meneliti dan mencegah serangan *brute force* dengan menggunakan *software Wireshark.*

Selain penelitian di atas, ada juga penelitian sebelumnya yang berjudul "*Investigating Brute force Attack Patterns in IoT Network*" yang dibuat oleh Deris Stiawan, Mohd. Yazid Idris, Reza Firsandaya Malik, Siti Nurmaini, Nizar Alsharif, Rahmat Budiarto pada tahun 2019, menjelaskan bahwa mereka meneliti tentang pola serangan *brute force* pada FTP *server* di jaringan IoT. Penelitian mereka berisi mendeteksi serangan *brute force* dan jenis serangan *brute force*

tersebut. Mereka tidak melakukan langkah pencegahan untuk menghentikan serangan *brute force* yang diterima.

Oleh karena itu, penulis berinisiatif untuk mengamankan data dari serangan *brute force* dan tidak menganalisanya saja menggunakan router mikrotik yang terdapat pada *server* jaringan di jurusan Teknik Komputer. Data yang akan diamankan oleh penulis adalah data *user* dan *password* pada *server* tersebut karena serangan *brute force* adalah serangan yang membobol *password user* dengan mencoba seluruh kemungkinan *password* sampai mendapatkan *password* yang sebenarnya. Penulis akan mencegah serangan *brute force* dengan cara melacak ip address penyerang dan memblokir *ip address* tersebut sesuai dengan waktu yang ditentukan (contohnya 1 hari). Berdasarkan latar belakang diatas, penulis mencoba membuat jaringan pada *server* aman dari serangan *brute force* dengan judul **"Implementasi Keamanan Jaringan Pada Router Mikrotik Terhadap Serangan *Brute force* Pada *Server* Jurusan Teknik Komputer"**

1.2 Rumusan Masalah

Berdasarkan uraian diatas, maka penulis merumuskan permasalahan yang ada yaitu bagaimana cara mengamankan *server* Jurusan Teknik Komputer terhadap serangan *brute force*.

1.3 Batasan Masalah

Agar penulisan laporan akhir dapat terarah dengan baik dan menghindari pembahasan yang jauh dari pokok permasalahan, maka penulis membatasi masalahan yaitu melakukan keamanan terhadap serangan *brute force* pada *server* jaringan dan menguji serangan *brute force* melalui OS Ubuntu.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Adapun tujuan dari penulisan proposal laporan akhir ini yaitu

1. Mengamankan *server* Teknik Komputer dari serangan *brute force.*
2. Memblokir *ip address* yang melakukan serangan *brute force*.

1.4.2 Manfaat

Manfaat dari penulisan laporan proposal laporan akhir ini yaitu

1. Memberikan keamanan pada *server* Teknik Komputer.
2. Agar tidak sembarang orang bisa mengakses *server* dengan cara melakukan serangan *brute force*.