BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komputerisasi yang begitu pesat yang sudah termasuk suatu kebutuhan di segala bidang menjadi salah satu hal yang menarik untuk dibahas. Tingkat keamanan yang tinggi mutlak seperti halnya kata sandi (*password*) yang merupakan metode autentikasi yang paling sering digunakan di berbagai sistem keamanan. Kemudahan dalam hal implementasi menjadi faktor utama dari pemanfaatan sistem berbasis *password*. Pengguna juga sudah terbiasa dengan sistem semacam ini sehingga waktu penyesuaian bisa diminimalkan. Autentikasi merupakan sebuah mekanisme yang digunakan untuk melakukan validasi terhadap identitas user yang mencoba mengakses sumber daya dalam sebuah sistem. Metode autentikasi konvensional yang selama ini familiar digunakan adalah menggunakan kombinasi "*username*" dan "*password*" atau biasa juga disebut dengan metode "*single factor authentication*". *Username* adalah sebuah penanda unik yang dapat digunakan untuk mengidentifikasi seorang user yang mencoba masuk (*log on*) kedalam sebuah sistem. *Password* adalah sebuah kombinasi rahasia yang terdiri dari kombinasi huruf, angka, dan karakter khusus. *Username* dan *password* di kombinasikan bersama-sama untuk mekanisme autentikasi pada sebuah sistem.

Di sisi lain, banyaknya penggunaan jaringan yang belum aman (misalnya protocol HTTP) masih menjadi ancaman bagi pengguna mengingat seringkali *password* menjadi satu-satunya mekanisme yang digunakan. Pemakaian satu metode (*one factor*) *password* dalam proses autentikasi memiliki banyak kelemahan, hal tersebut terbukti dari banyak kasus yang terjadi. Ketika *username* dan *password* seseorang sudah diketahui oleh penyerang maka tidak ada mekanisme berikutnya yang dapat menghalangi akses yang di lakukan oleh seorang penyerang terhadap sistem. Mengapa kombinasi *username* dan *password* ini rentan terhadap serangan oleh pengacau? Hal ini karena masih banyak organisasi atau individu yang belum menerapkan kebijakan *username* dan *password* yang aman.

Sehingga jenis serangan seperti *brute force attack* dan *social engineering* sangat mudah menjebol mekanisme autentikasi tunggal ini.

Brute Force Attack adalah serangan yang dilakukan untuk membobol *password* dengan cara mencoba setiap *password* sampai akhirnya menemukan *password* yang tepat. Peretas akan menggunakan algoritma yang menggabungkan huruf, angka dan simbol untuk menghasilkan *password* untuk serangan tersebut. *Social engineering* adalah manipulasi psikologis dari seseorang dalam melakukan aksi atau menguak suatu informasi rahasia. Umumnya dilakukan melalui telepon atau internet. *Social engineering* merupakan salah satu metode yang digunakan oleh hacker untuk memperoleh informasi tentang targetnya, dengan cara meminta informasi itu langsung kepada korban atau pihak lain yang mempunyai informasi itu.

Oleh karena itu, selain menggunakan teknik enkripsi *password* yang handal, dibutuhkan juga kekuatan dari metode autentikasinya. Sehingga tidak hanya pencapaian aspek kerahasiaannya (*privacy/confidentiality*) dan keutuhan data (*integrity*) saja yang diproteksi, tetapi juga jaminan keabsahan akses yang telah dilakukan user (*nonrepudiation*). Tujuan utama autentikasi adalah pembuktian identitas *user*, apakah sah terdaftar atau tidak. Metode yang digunakan dalam autentikasi adalah *two factor authentication* (TFA/2FA) dimana dua faktor yang bersifat independen akan digunakan dalam membuktikan adanya klaim bahwa sebuah entitas atau identitas itu asli. Dengan menggunakan TFA, maka *password* bukan menjadi *single point attack* dalam hal akses kepada identitas pengguna. Banyak perusahaan besar telah menggunakan TFA sebagai tambahan pengamanan terhadap serangan brute-force terhadap *password*, seperti Google, Twitter, dan Facebook.

Dari sedikit penjelasan yang dikemukakan diatas, maka penulis akan mengimplementasikan *two factor authentication* agar dapat meningkatkan keamanan terhadap sistem *login* administrator *website* tv.polsri.ac.id sehinga laporan akhir ini berjudul **"Implementasi Sistem *Two Factor Authentication* Untuk Meningkatkan Keamanan *Login* Administrator Pada *Website* TVPOLSRI"**

1.2 Rumusan Masalah

Dengan mengacu pada latar belakang diatas, maka dapat dirumuskan masalah yang akan dibahas dalam laporan akhir ini, yaitu bagaimana mengimplementasikan *two factor authentication* pada sistem *login* administrator *website* tv.polsri.ac.id sehingga sistem dapat menghalangi atau menyangkal aktifitas *login* identitas *user* yang illegal atau tidak sah. Dan bagaimana administrator atau *user* yang tepat mendapat kode yang dibutuhkan untuk melakukan *login*.

1.3 Batasan Masalah

Penyusunan laporan akhir ini agar terarah dan tidak menyimpang dari permasalahan yang akan dibahas maka diperlukan untuk membatasi masalah melliputi:

1. Tentang *two factor authentication login* administrator yang membutuhkan verifikasi tambahan yang berupa kode 6 digit angka, selain *username* dan *password*.
2. Menggunakan *Simple Mail Transfer Protocol* (SMTP) yang diperuntukkan untuk mengirim mail berisikan kode verifikasi kepada *user* yang asli.
3. Sistem yang hanya digunakan dalam lingkungan kampus Politeknik Negeri Sriwijaya dan tidak melakukan mekanisme penyerangan (*intruder*) seperti *bruce force attack* dan lain sebagainya

1.4 Tujuan

Dari permasalahan diatas, maka tujuan yang ingin dicapai dari tugas akhir adalah sebagai berikut:

1. Dapat mengetahui cara kerja *two factor authentication* yang di aplikasikan atau diimplementasikan ke sistem *login* administrator *website* tv.polsri.ac.id
2. Memastikan dengan benar adanya hasil kinerja sistem *login two factor authentication* tersebut dan dapat didemonstrasikan langsung. Serta benar-benar dapat dipergunakan sebagaimana mestinya.

1.5 Manfaat

Adapun manfaat yang diharapkan dari tugas akhir ini adalah sebagai berikut:

1. Meningkatkan keamanan terhadap sistem *login* administrator *website* tv.polsri.ac.id termasuk menjaga aspek kerahasiaan (*privacy /confidentiality*), keutuhan data (*integrity*) yang diproteksi, dan juga jaminan keabsahan akses yang telah dilakukan administrator.
2. Sebagai bahan acuan bagi pembaca khususnya mahasiswa Jurusan Teknik Komputer dan pihak yang berkaitan agar selanjutnya dapat dikembangkan.