BAB I
PENDAHULUAN

1.1 Latar Belakang

Jurusan Teknik Komputer merupakan salah satu jurusan Perguruan Tinggi Negeri di Politeknik Negeri Sriwijaya. Keamanan jaringan merupakan yang penting untuk diperhatikan oleh sebuah Perguruan Tinggi. Semakin banyaknya pengguna layanan *internet working* maka semakin banyak pula permasalahan dan kendala yang dihadapi didalam dunia teknologi jaringan komputer. *Wireless* LAN berbasis 802.11 telah menjadi hal yang umum di lingkungan perkantoran dan kampus . Pada jaringan nirkabel, masalah keamanan memerlukan perhatian yang lebih serius, mengingat media transmisi datanya adalah gelombang radio yang bersifat *broadcast*.

Di jurusan Teknik Komputer keamanan jaringan *wireless* masih menggunakan WEP, WPA, WPA2, dan *Hotspot login*, yang dimana untuk mengaksess jaringan *wireless* tersebut hanya dengan memasukkan *password* yang di tentukan oleh administrator jaringan sehingga siapa saja yang mengetahuinya bisa mengakses jaringan *wireless* tersebut dengan tanpa hambatan. Diperlukan sistem keamanan untuk mencegah bebasnya akses jaringan *wireless* ini di jurusan Teknik Komputer. Banyak penyedia jasa *wireless* seperti hotspot komersil, ISP, Warnet, kampus-kampus maupun perkantoran sudah mulai memanfaatkan *wireless* pada jaringan masing masing, tetapi sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan *wireless* tersebut. Hal ini membuat para *hacker* menjadi tertarik untuk meng-*explore* keamampuannya untuk melakukan berbagai aktifitas yang ilegal dengan menggunakan *Wi-Fi* yang tersedia. Kelemahan jaringan *wireless* secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Salah satu contoh penyebab kelemahan pada konfigurasi karena saat ini untuk membangun sebuah jaringan *wireless* cukup mudah. Banyak vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan *wireless* yang masih menggunakan konfigurasi *wireless default* bawaan vendor. Sering

sekali ditemukan *wireless* yang dipasang pada jaringan masih menggunakan *setting default* bawaan vendor seperti SSID, IP *Address*, *remote managment*, DHCP *enable*, kanal frekuensi yang tidak terenkripsi, dan bahkan tanpa *user*/*password* untuk administrasi *wireless* tersebut. Untuk memilimalisir pengguna layanan jaringan tanpa membatasi akses kedalam jaringan dapat menggunakan sistem keamanan MAC *Address Filtering*.

Berdasarkan penjelasan di atas, sehingga dipandang perlu mencari alternatif untuk meningkatkan keamanan jaringan, salah satunya dengan menggunakan cara *two factor*, *password* dan *filtering* MAC *address*. MAC *address filtering* merupakan metode *filtering* untuk membatasi hak akses dari MAC *Address* yang bersangkutan dan juga penulis merancang aplikasi keamanan data *user* yang berguna untuk membatasi dan menciptakan keamanan data pengguna yang akan mengakses jaringan *wireless* di jurusan Teknik Komputer. Berdasarkan latar belakang yang telah dijelaskan maka penulis membuat laporan akhir yang berjudul "**APLIKASI KEAMANAN DATA *USER* DAN SISTEM KEAMANAN *WIRELESS* MENGGUNAKAN *TWO FACTOR, PASSWORD* DAN MAC *ADDRESS FILTERING* DI JURUSAN TEKNIK KOMPUTER**".

1.2 Rumusan masalah

Berdasarkan latar belakang di atas adapun rumusan masalah yang di dapat yaitu **dilakukan pengaturan keamanan *wireless* dan membuat aplikasi keamanan data *user* berbasis web untuk membatasi pengguna jaringan *wireless* menggunakan keamanan pada WPA-PSK dan MAC *Address filtering*.**

1.3 Batasan Masalah

Agar penulisan Laporan Akhir ini lebih terarah dan tidak menyimpang dari permasalahan yang ada, maka penulis membatasi pokok permasalahan sebagai berikut :

1. Sistem yang dibuat membantu dalam menyimpan data pengguna yang pernah dan akan mendaftar ke jaringan *wireless*.
2. Sistem yang dibangun berbasis web dengan menggunakan bahasa

pemrograman PHP serta dengan menggunakan basis data MySQL

3. Alat yang digunakan yaitu Mikrotik Router RBD52G-5HacD2HnD-TC.
4. Pengintergrasian mikrotik dengan memanfaatkan Winbox.
5. Keamanan yang digunakan yaitu dengan menggunakan *setting*-an pada *firewall* yaitu pada *filter rules* dan NAT.

1.4 Tujuan

Tujuan dari pembuatan laporan ini yaitu:

1. Menciptakan sistem keamanan pada mikrotik untuk mengatur keamanan wireless menggunakan WPA-PSK dan MAC *Address filtering* dan *setting*-an pada *firewall* yaitu pada *filter rules* dan NAT.
2. Merancang aplikasi keamanan data *user* berbasis web di jurusan Teknik Komputer menggunakan CodeIgniter.

1.5 Manfaat

Manfaat yang diharapkan oleh penulis apabila tujuan penyusunan laporan akhir ini tercapai yaitu:

1. Data pengguna *wireless*/hotspot disimpan di aplikasi keamanan data user berbasis web yang memiliki keamanan yang baik.
2. Data pengguna *wireless*/hotspot menggunakan sistem autentikasi 2 faktor dengan *firewall filtering* MAC *Address* sehingga memiliki keamanan yang lebih baik.

Agar terciptanya sistem keamanan jaringan komputer menggunakan *firewall* mikrotik