

# **BAB I**

## **PENDAHULUAN**

### **1.1. LATAR BELAKANG MASALAH**

Perkembangan teknologi informasi saat ini semakin maju terutama di bidang keamanan jaringan komputer. Keamanan Komputer sangatlah penting karena menjaga agar suatu hal tidak rusak atau hilang. Keamanan Komputer dapat menjaga suatu perangkat komputer agar tetap aman dari *malware* yang merusak ataupun dari aksi pencurian data – data yang bersifat privasi yang hanya pemilik dari data tersebut yang dapat mengakses. Sistem Keamanan Komputer meliputi banyak hal seperti: Keamanan Jaringan, Keamanan Data dan Keamanan Sistem[1].

Pajak adalah kontribusi wajib kepada negara yang terutang oleh orang pribadi atau badan yang bersifat memaksa berdasarkan Undang-Undang, dengan tidak mendapatkan imbalan secara langsung dan digunakan untuk keperluan negara bagi sebesar-besarnya kemakmuran rakyat. [2].

Kantor Konsultan Pajak Edi Kurniawan Ini beralamatkan di Jl. Kapt. Pattimura No. 85, Simp STM Atas, Kel. Simp IV Sipin, Kec. Telanai Pura, Kota Jambi, Provinsi Jambi. KKP ini menyediakan konsultasi perpajakan, perencanaan perpajakan dan membantu pembuatan laporan perpajak para wajib pajak pribadi maupun wajib pajak badan.

Layanan perpajakan disaat ini sangat dipermudah karena sekarang wajib pajak tidak perlu lagi untuk ke kantor pajak, direktorat jendral pajak telah memanfaatkan perkembangan teknologi yang ada saat ini dengan menghadirkan sistem pelaporan

yang berbasis *online* atau daring melalui situs *djp online*. Disitus ini wajib pajak dapat melakukan pelaporan perpajakan serta pembuatan *billing* pembayaran pajak, hingga masih banyak lagi layanan yang ada disitus ini.

Pemanfaatan jaringan komputer di era sekarang khususnya pada pelaporan perpajakan saat ini sangatlah mempermudah wajib pajak yang ingin melakukan pembayaran hingga pelaporan perpajakan, sehingga tidak menutup kemungkinan adanya celanya penyusupan untuk pencurian data wajib pajak pada jaringan yang ada di kantor konsultan pajak Edi Kurniawan dikarenakan belum adanya sistem pengamanan jaringan komputer yang cukup untuk mengamankan jaringan komputer yang ada di kantor ini, pengamanan yang digunakan saat ini hanya memanfaatkan keamanan yang ada pada penyedia layanan internet saja .

Dengan adanya pemanfaatan jaringan komputer pada sistem perpajakan ini, tidak menutup kemungkinan akan terjadi pencurian atau pembobolan data pada jaringan komputer yang terhubung ke server sistem *djp online*, misalnya admin sedang memasukkan laporan SPT tahunan badan yang di akses melalui sistem *djp online* bisa saja dalam pengaksesan sistem *djp online* dengan jaringan yang belum menyediakan layanan keamanan dapat terjadi pencurian data yang tidak di ketahui oleh admin atau karyawan yang ada di kantor tersebut, sehingga diperlukannya sistem keamanan jaringan komputer yang dapat menjadi solusi dalam pencegahan terjadinya pencurian data yang dianggap rahasia ini.

Pada penelitian sebelumnya yang di lakukan oleh Noviar Armanda Nurdin, Septian Ardiansyah [3] metode yang digunakan adalah *MAC Address filtering* pada jaringan yang ada pada PT Pertamina Drilling Service Indonesia, hasil dari

penelitian ini adalah *filtering MAC Address* untuk menambah keamanan jaringan pada PT PDSI sehingga user lain tidak dapat mengakses melalui *device* lain sehingga keamanan lebih terjamin. Menurut Slamet Widodo et al. [4] metode yang digunakan *Two Factor, Password* dan *MAC Address Filtering*, Dengan adanya aplikasi keamanan data user berbasis web ini memudahkan operator jaringan untuk mendaftarkan *MAC Address* mahasiswa dan pengguna wireless di jurusan Teknik Komputer, sehingga meminimalisir terjadinya penyalahgunaan hak akses jaringan *wireless* di jurusan Teknik Komputer. Menurut Syaiful dan Cahyuni Novia [5] metode yang digunakan pada penelitian adalah *Hotspot* dan *MAC Address Filtering*, dengan memanfaatkan fitur *access list* dan *connect list* pada mikrotik dapat melihat *user* yang terkoneksi ke jaringan komputer serta menjadi parameter untuk memonitoring seperti kekuatan sinyal dan juga dapat melihat *wireless protocol* yang digunakan oleh *user*, selain itu fungsi dari *access list* adalah mencegah agar user yang tidak terdaftar alamat *MAC* nya tidak dapat terkoneksi ke jaringan komputer.

Melihat dari hasil penelitian sebelumnya yang dilakukan oleh peneliti sebelumnya penulis menyarankan untuk menggunakan metode *Hotspot* dan *MAC Address Filtering* yang dikira cocok untuk mengamankan jaringan *Wireless* yang ada pada Kantor Konsultan Pajak Edi Kurniawan. Pemilihan dua metode ini untuk mengamankan jaringan *wireless* yang ada pada Kantor Konsultan Pajak Edi Kurniawan adalah jaringan *wireless* yang ada saat ini belum memiliki sistem keamanan yang dapat menjadi solusi untuk permasalahan keamanan jaringan *wireless* yang ada pada Kantor Konsultan Pajak Edi Kurniawan.

Berdasarkan permasalahan yang ada penulis tertarik untuk melakukan penelitian yang di tuangkan dalam bentuk laporan tugas akhir dengan mengangkat sebuah judul “**PERANCANGAN SISTEM KEAMANAN JARINGAN WIRELESS PADA KANTOR KONSULTAN PAJAK EDI KURNIAWAN**”.

## **1.2. RUMUSAN MASALAH**

Dari latar belakang masalah yang telah diuraikan ini, maka rumusan masalah yang akan dibahas adalah bagaimana merancang sistem keamanan jaringan *wireless* pada KKP Edi Kurniawan Jambi.

## **1.3. BATASAN MASALAH**

Untuk menghindari pembahasan diluar judul penelitian, maka penulis melakukan pembahasan yang lebih spesifik berdasarkan judul tersebut. Adapun batasan masalahnya mencakup :

1. Sistem keamanan jaringan ini digunakan untuk memperkuat pengamanan data perpajakan yang dimiliki para klien konsultan pajak Edi Kurniawan.
2. Alat yang akan digunakan dalam penelitian ini adalah Mikrotik RB-941 hAP.
3. Penerapan metode *MAC Address Filtering* pada fitur *hotspot*.
4. Metode *Wireless Security Key* yang digunakan adalah WPA2/AES.

## **1.4. TUJUAN PENELITIAN**

Adapun tujuan penulis melakukan penelitian ini adalah Merancang sebuah sistem keamanan jaringan *wireless* pada KKP Edi Kurniawan.

## 1.5. MANFAAT PENELITIAN

Adapun manfaat dari penelitian ini adalah sebagai berikut :

1. Dengan adanya fitur hotspot ini dapat membantu memperkuat lagi sistem keamanan yang ada pada KKP Edi Kurniawan.
2. Menggunakan fitur *Hotspot* dan *MAC Address Filtering* ini dapat menjadi pengamanan ganda untuk jaringan yang ada di Kantor Konsultan pajak Edi Kurniawan

## 1.6. SISTEMATIKA PENULISAN

Untuk memberikan gambaran umum mengenai keseluruhan penulisan ilmiah, dapat dilihat melalui sistematika penulisan yang meliputi :

### **BAB I : PENDAHULUAN**

Bab ini menguraikan tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan.

### **BAB II : LANDASAN TEORI**

Pada bab ini merupakan bab yang berisikan tentang uraian konsep-konsep teoritis yang mendasari penelitian dan teori teori yang relevan untuk menyelesaikan masalah penelitian secara khusus digunakan sebagai landasan untuk menjawab masalah penelitian.

### **BAB III : METODOLOGI PENELITIAN**

Dalam bab ini dijelaskan tahapan proses yang dilakukan selama mengerjakan penelitian, metode yang digunakan dan tools yang digunakan untuk analisis dalam proses penelitian.

#### **BAB IV : ANALISA DAN PERANCANGAN SISTEM**

Dalam bab ini dijelaskan mengenai gambaran umum dan analisis untuk kondisi dan penggunaan jaringan yang ada di Kantor Konsultan Pajak Edi Kurniawan yang sedang berjalan saat ini.

#### **BAB V : IMPLEMENTASI DAN PENGUJIAN**

Dalam bab ini dijelaskan mengenai kegiatan implementasi terhadap sistem yang telah dibangun, hal-hal mengenai kelebihan dan kekurangan dalam sistem, dan analisis hasil yang dicapai dalam sistem tersebut.

#### **BAB VI : PENUTUP**

Bab ini berisikan kesimpulan dan dari penelitian yang telah dilakanakan beserta saran yang berguna untuk pengembangan penelitian selanjutnya.