

BAB I

PENDAHULUAN

1.1 Latar Belakang

Salah satu perubahan utama di bidang telekomunikasi adalah penggunaan teknologi *wireless*. Teknologi *wireless* juga diterapkan pada jaringan komputer, yang lebih dikenal dengan *wireless* LAN atau WLAN. Penggunaan *wireless* LAN menjadi daya tarik tersendiri bagi para pengguna komputer menggunakan teknologi ini untuk mengakses suatu jaringan komputer atau informasi (internet). Pengguna teknologi *wireless* LAN mengalami peningkatan yang pesat seiring dengan peningkatan jumlah *hotspot* di tempat-tempat umum, seperti restoran, mall, perkantoran bahkan juga di kampus dan di sekolah-sekolah. Teknologi *wireless* menawarkan beragam kemudahan, kebebasan dan fleksibilitas yang tinggi. Teknologi *wireless* memiliki cukup banyak kelebihan dibandingkan teknologi kabel yang sudah ada. Teknologi *wireless* sangat mudah untuk digunakan dan pengguna bisa saling berkomunikasi antar jaringan selama masih berada dalam jangkauan *wireless*.

Kantor Perkebunan PTPN 7 Musi Landas untuk keamanan jaringan *wireless* masih menggunakan metode *WEP/WPA/WPA2*, hampir semua pengguna jaringan *wireless* rata-rata mengimplemetasikan perangkat *access point* nya dengan menggunakan metode tersebut. Metode tersebut dikenal

baik dalam hal kemampuan pengamanan *security* jaringan *wireless* tetapi metode *WEP/WPA/WPA2* masih bisa ditembus oleh *software hacking* dengan metode *brute-force attack* dan *dictionary*, dimana *software* tersebut banyak terdapat di internet dan kelemahan berikutnya adalah metode tersebut hanya menggunakan *password* saat akan terkoneksi perangkat *access point* sehingga *password* tersebut mudah tersebar jika salah satu *user* memberi *password* nya kepada *user* lain dan dengan mudah diketahui oleh *user* lain begitu seterusnya. Oleh karena itu diperlukan sebuah sistem yang dapat meningkatkan sistem keamanan *wireless hotspot*.

Salah satu solusi keamanan *wireless hotspot* yang akan diterapkan di Kantor Perkebunan PTPN 7 Musi Landas adalah dengan menerapkan Metode SSL (*Secure Socket Layer*). Metode SSL (*Secure Socket Layer*) telah banyak digunakan untuk pengamanan *website* yang membutuhkan pengamanan tingkat tinggi seperti *website* perbankan, *hosting*, jual beli *online* dan sebagainya yang biasanya pada *website* tersebut menggunakan *protocol HTTPS (Hyper Text Transfer Protocol Secure)*. Implementasi *server gateway* yang berfungsi sebagai *router internet* baik pada jaringan kabel maupun *wireless*. Hal ini menjadi sebuah solusi dimana dapat membantu komunikasi antar komputer serta sistem keamanan *internet hotspot* dimana pengguna akan melakukan proses *login* terlebih dahulu dengan memasukkan nama *user* dan *password* saat akan mengakses internet dengan menggunakan metode keamanan *Secure Socket Layer (SSL)*.

Berdasarkan latar belakang di atas, penulis tertarik untuk membuat

penelitian dengan judul **Analisis Keamanan Jaringan Hotspot Menggunakan Metode *Security OpenSSL (Secure Socket Layer)* Pada Kantor Perkebunan PTPN 7 Musi Landas.**

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka dapat dirumuskan permasalahan yang ada yaitu, bagaimana mengimplementasikan dan menganalisis sistem keamanan internet hotspot dengan menggunakan metode SSL (*Secure Socket Layer*) di Kantor Perkebunan PTPN 7 Musi Landas?

1.3 Ruang Lingkup

Agar permasalahan lebih terarah dan tidak menyimpang, maka perlu adanya batasan masalah. Adapun batasan masalah pada penelitian ini adalah mengimplementasikan dan menganalisis sistem keamanan *wireless internet hotspot* dengan metode *Secure Socket Layer (SSL)* di Kantor Perkebunan PTPN 7 Musi Landas dengan menggunakan metode penelitian *Action Research*.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan Penelitian

Adapun Tujuan penelitian ini adalah sebagai berikut :

1. Untuk merancang dan menganalisis sistem keamanan *wireless internet hotspot* dengan menggunakan *security Secure Socket Layer (SSL)* dengan

menggunakan *algoritma enkripsi simetrik* berupa sertifikat digital dan *public key* di Kantor Perkebunan PTPN 7 Musi Landas.

2. Untuk mendapatkan hasil analisis pengujian penetrasi sistem keamanan *wireless internet hotspot* dengan menggunakan *security Secure Socket Layer (SSL)* dengan menggunakan *algoritma enkripsi simetrik* berupa sertifikat digital dan *public key*.

1.4.2 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut :

- a. Membantu kemudahan dan menjaga keamanan dalam mengakses *internet* bagi pengguna dalam memperoleh informasi internet dengan menggunakan perangkat *laptop, handphone, perangkat mobile* lainnya menggunakan fasilitas *wifi* atau *hotspot internet*.
- b. Dari hasil penelitian ini diharapkan dapat diketahui kelebihan dan kekurangan sistem keamanan *security Secure Socket Layer (SSL)* yang dibangun.
- c. Dari penelitian ini diharapkan dapat menambah pengetahuan dan pengalaman dalam menganalisis sehingga dapat menambah ilmu pengetahuan serta bisa mengembangkan ilmu pengetahuan yang didapat dalam perkuliahan serta diharapkan dapat menjadi bahan referensi untuk mahasiswa Universitas Bina Darma Palembang untuk penelitian selanjutnya.

1.5 Metodologi Penelitian

Metode penelitian yang akan digunakan adalah metode *action research*. Menurut Kock (2007:45), Metode *Action Research* merupakan penelitian tindakan. Metode *action research* penelitian yang bersifat partisipatif dan kolaboratif. Maksudnya penelitiannya dilakukan sendiri oleh peneliti, dengan penelitian tindakan. *Action research* dibagi dalam beberapa tahapan yang merupakan siklus, yaitu :

a. Tahap pertama (*Diagnosing*)

Pada tahap ini peneliti mengidentifikasi masalah pada jaringan *wireless* di Kantor Perkebunan PTPN 7 Musi Landas. Untuk keamanan jaringan *wireless* pada perangkat *access point* metode *security* yang masih digunakan adalah metode WEP/WPA/WPA2. Metode tersebut dikenal baik dalam hal kemampuan pengamanan *security* jaringan *wireless* tetapi metode WEP/WPA/WPA2 masih bisa ditembus oleh *software hacking*/penyusup, dimana aplikasi tersebut banyak terdapat di internet dan kelemahan berikutnya adalah metode tersebut hanya menggunakan *password* saat akan terkoneksi perangkat *access point* sehingga *password* tersebut mudah tersebar dan dengan mudah diketahui oleh pengguna lain serta penggunaan user tanpa batas.

b. Tahap kedua (*Action Planning*)

Peneliti memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan

masalah yang ada, pada tahap ini penulis memasuki tahapan persiapan *hardware* dan *software* pengujian serta topologi jaringan.

c. Tahap ketiga (*Action Taking*)

Peneliti mengimplementasikan rencana tindakan dengan harapan dapat menyelesaikan masalah. Selanjutnya dengan model dibuat berdasarkan sketsa infrastruktur jaringan *wireless* dilanjutkan dengan melakukan analisis terhadap sistem yang sedang berjalan dengan melakukan proses pengambilan data *screen shot* dan analisa sistem keamanan *wireless hotspot* dengan metode *security Secure Socket Layer (SSL)* menggunakan aplikasi *wireshark*.

d. Tahap keempat (*Evaluating*)

Setelah melakukan tahapan implementasi dan pengujian serta mendapatkan hasil pengujian, proses selanjutnya melakukan evaluasi dan analisis terhadap hasil yang didapat.

e. Tahap kelima (*Learning / Reflecting*)

Setelah semuanya selesai, maka tahap akhir adalah peneliti melaksanakan *review* dan *evaluasi* tahap demi tahap kemudian penelitian ini dapat berakhir. Hasilnya juga mempertimbangkan untuk tindakan kedepan.

1.6 Sistematika Penulisan

Skripsi ini ditulis dalam lima bab dan masing-masing bab terbagi dalam sub-sub bab. Sistematika penulisan disusun sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini Penulis akan menguraikan tentang latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini menjelaskan pembahasan mengenai landasan teori yaitu mengenai teori-teori yang berkaitan dengan pokok permasalahan dalam penelitian.

BAB III METODOLOGI PENELITIAN

Dalam bab ini membahas analisis kebutuhan *hardware* dan *software*, metode penelitian dan jadwal penelitian.

BAB IV HASIL DAN PEMBAHASAN

Dalam bab ini membahas mengenai implementasi dan analisis pengujian data hasil penelitian yang telah dilakukan berupa hasil penetrasi keamanan serta pembahasan.

BAB V KESIMPULAN DAN SARAN

Menguraikan beberapa kesimpulan dari pembahasan masalah dari bab-bab sebelumnya serta memberikan saran yang bisa bermanfaat.

