BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi *Wireless Fidelity* (Wi-Fi) merupakan salah satu contoh dari jaringan *wireless*. Wi-Fi adalah sekumpulan standar yang digunakan untuk jaringan lokal nirkabel (*Wireless* Local Area Network-WLAN) [1]. Wi-Fi merupakan koneksi tanpa kabel untuk saling bertukar data menggunakan gelombang radio dengan peralatan elektronik. Kegunaan Wi-Fi tidak hanya untuk mengakses internet saja tapi juga dapat digunakan untuk membuat jaringan nirkabel pada suatu lembaga. Oleh karena itu, banyak lembaga yang memanfaatkan Wi-Fi sebagai sarana akses internet kepada karyawan, anggota, atau pengunjung untuk mengakses atau mentransfer data secara mudah.

Penggunaan Wi-Fi semakin meningkat baik untuk tujuan pendidikan maupun komersial. Jaringan Wi-Fi menawarkan banyak kemudahan dalam penggunaannya, namun hal tersebut tidak dapat menjamin pengguna aman dari serangan pihak yang tidak bertanggung jawab seperti hacker yang bisa mengeksploitasi data penting dari suatu instansi, menyadap data seperti *username* atau *password* dan mengubah data penggunanya. Oleh karena itu dibutuhkan perancangan sistem keamanan jaringan Wi-Fi dengan teliti agar meminimalisir segala jenis serangan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab untuk dapat melindungi pengguna Wi-Fi [2]. Secara garis besar, celah jaringan *wireless* mencakup empat layer, yaitu Physical Layer, Network Layer, User Layer dan Application Layer, yang sebenarnya merupakan proses komunikasi data pada media *wireless*. Hal ini membua para

hacker menjadi tertarik untuk melakukan berbagai aktivitas ilegal dengan menggunakan kemampuanya dalam melakukan penyerangan terhadap jaringan Wi-Fi.

Kelemahan jaringan *wireless* secara umum dibagi menjadi 2 jenis, yaitu kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi [3]. Salah satu penyebab dari kelemahan konfigurasi adalah pemasangan sebuah jaringan *wireless* yang tidak memerhatikan keamanan. Biasanya pemasangan hanya dilakukan menggunakan konfigurasi *wireless* bawaan dari penyedia layanan tanpa enkripsi untuk log in atau masuk ke jaringan wifi tersebut sehingga keamanan pada suatu jaringan *wireless* tidak maksimal [4].

Undang-undang Republik Indonesia Nomor. 11 tahun 2008 tentang informasi dan transaksi elektronik sudah diatur dalam bab VII perbuatan yang dilarang, pasal 30 ayat (3), menyatakan bahwa “Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan”. Seiring berkembangnya teknologi, serangan jaringan Wi-Fi dapat terjadi dimana saja, termasuk Indonesia. Terdapat beragam jenis serangan jaringan Wi-Fi, seperti serangan sniffing (pencurian data), serangan DoS (Denial of Service), serangan phising (penipuan online), dan serangan terhadap kerentanan tertentu dalam protokol Wi-Fi. Adapun beberapa contoh kerugian yang dapat terjadi akibat serangan jaringan Wi-Fi di Indonesia, salah satunya adalah kebocoran data yang dijelaskan pada situs Badan Siber dan Sandi Negara RI yang terjadi pada beberapa sektor seperti pemerintah, keuangan, telekomunikasi, penegakan hukum, transportasi, BUMN dan lainnya yang menyebabkan kerugian besar. Rumah Sakit Umum Daerah (RSUD) dr. Soedono Provinsi Jawa Timur merupakan fasilitas kesehatan yang memberikan pelayanan medis dan administrasi kepada pasien. Seiring dengan kemajuan teknologi informasi, RSUD juga

memanfaatkan jaringan Wi-Fi dalam penyediaan akses informasi yang cepat dan efisien untuk mendukung banyak aspek operasionalnya. Namun disisi lain penggunaan jaringan Wi-Fi dapat menimbulkan celah keamanan jaringan yang memengaruhi kerahasiaan, keintegritasan, dan ketersediaan data penting.

Percobaan pembobolan jaringan Wi-Fi pernah terjadi di RSUD dr. Soedono Provinsi Jawa Timur, hal tersebut disampaikan oleh pihak Instalasi Teknologi Informasi dan Sistem Informasi (ITISI), namun percobaan tersebut berhasil digagalkan. Pihak ITISI RSUD dr. Soedono Provinsi Jawa Timur juga mengatakan bahwa jaringan *wireless* sudah dilakukan perbaikan berupa melakukan update pada *firmware* Wi-Fi, mengganti password Wi-Fi yang lama dan melakukan konfigurasi ulang pada *firewall* untuk meningkatkan keamanannya. Akan tetapi, jaringan Wi-Fi RSUD dr. Soedono Provinsi Jawa Timur setelah dilakukan perbaikan belum pernah dilakukan pengujian untuk diketahui celah keamanannya.

Penetration testing adalah suatu metode yang dapat dimanfaatkan untuk melakukan pengujian terhadap kelemahan sistem komputer, jaringan atau aplikasi web. Pengumpulan data kerentanan atau celah keamanan diperlukan dalam metode *Penetration testing* sebagai tolak ukur untuk memperbaiki dan meningkatkan keamanan web server. *Penetration testing* memiliki tiga strategi yang dapat dilakukan antara lain *Black Box Testing*, *White Box Testing*, dan *Gray Box Testing*. Dari uraian yang telah dijelaskan di atas, maka penelitian ini akan melakukan pengujian dan analisis terhadap keamanan jaringan Wi-Fi RSUD dr. Soedono Provinsi Jawa Timur menggunakan metode *Penetration testing*.

1.2 Batasan Masalah

Berdasarkan identifikasi masalah diatas, maka batasan masalah pada penelitian ini adalah sebagai berikut:

1. Melakukan pengujian *Penetration testing* dengan empat jenis serangan yaitu: *Cracking The Encryption, Bypassing MAC Authentication, Attacking The Infrastructure, dan Man In The Middle* Attack terhadap jaringan Wi-Fi rumah sakit untuk menganalisis celah keamanan
2. Penulis tidak melakukan implementasi peningkatan jaringan, hanya melakukan analisis pada jaringan dan memberikan solusi kepada pihak ITISI untuk mengamankan jaringan

1.3 Rumusan Masalah

Berdasarkan pemaparan latar belakang diatas, maka dapat dirumuskan suatu masalah yaitu:

1. Bagaimana pengujian celah keamanan jaringan Wi-Fi RSUD dr. Soedono Provinsi Jawa Timur menggunakan metode *Penetration testing*?
2. Bagaimana analisis keamanan jaringan Wi-Fi RSUD dr. Soedono Provinsi Jawa Timur?

1.4 Tujuan Penelitian

Berdasarkan uraian rumusan masalah diatas, tujuan yang hendak dicapai dalam penelitian ini adalah:

Mengetahui celah keamanan yang ada pada jaringan *wireless* di RSUD dr. Soedono Provinsi Jawa Timur

1. Menganalisa tingkat keamanan jaringan Wi-Fi di RSUD dr. Soedono Provinsi Jawa Timur terhadap serangan luar atau dalam

1.5 Manfaat Penelitian

Manfaat yang diharapkan didapatkan dari penelitian yang dilakukan ini adalah sebagai berikut:

1. Sebagai gambaran dasar dalam memberikan solusi untuk peningkatan keamanan jaringan Wi-Fi RSUD dr. Soedono Provinsi Jawa Timur
2. Mengetahui tingkat keamanan dari jaringan Wi-Fi RSUD dr. Soedono Provinsi Jawa Timur dari serangan luar atau dalam