

## BAB I PENDAHULUAN

### 1.1 Latar Belakang

Keamanan informasi menjadi hal yang sangat penting bagi sebuah instalasi ataupun organisasi yang sudah memiliki jaringan komputer ataupun jaringan internet untuk menunjang kualitas pelayanan yang lebih efektif dan efisien. Pentingnya sebuah informasi harus didukung dengan sistem keamanan yang tinggi, agar tidak menimbulkan kerugian bagi instalasi maupun masyarakat. Dalam pembangunan perancangan, sistem keamanan jaringan yang terhubung ke internet harus dirancang dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh para *hacker*.

*Wirshark* adalah *tools packet sniffer* yang digunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan. Alat ini memiliki kemampuan untuk memblokir lalu lintas pada jaringan LAN, mencuri *password*, dan melakukan penyadapan aktif terhadap protokol-protokol umum. Sedangkan *Netstumbler* adalah *tools wifi hacking* yang digunakan untuk mendeteksi dan mengidentifikasi sinyal *wireless* yang terbuka dan menyusup kedalam jaringan.

Dalam hal ini, diperlukan adanya analisis terhadap keamanan jaringan *area* yang terdapat di sekitar. Jaringan *area* yang sering ditemukan adalah salah satu produk layanan berupa paket layanan komunikasi dan data seperti telepon rumah (*voice*), internet (*internet on fiber* atau *High Speed Internet*), dan layanan televisi interaktif. *Packet Sniffing* adalah sebuah teknik pencurian data yang dilakukan dengan cara memonitor atau melakukan analisis terhadap paket data

yang ditransmisikan dari komputer *client* ke *web server*. Dengan menggunakan metode tersebut diharapkan memperoleh solusi terbaik dari masalah yang dihadapi.

Berdasarkan uraian diatas, penulis tertarik untuk mempelajari cara untuk mengamankan suatu jaringan. Oleh karena itu, penulis mengambil bahan mengenai keamanan jaringan internet dengan judul **"Anallsis Keamanan Jaringan (Wifi) Terhadap Serangan *Packet Sniffing*."**

### **1.2 Rumusan Masalah**

Berdasarkan latar belakang masalah yang telah diuraikan sebelumnya maka dapat diperoleh rumusan masalah sebagai berikut:

"Bagaimana meningkatkan keamanan jaringan *wifi*?"

### **1.3 Batasan Masalah**

Untuk menegaskan penelitian ini, maka dibuat beberapa batasan masalah sebagai berikut:

1. Penggunaan aplikasi *Wireshark*, dan *inSSIDer* untuk menganalisa keamanan jaringan (*wifi*).
2. Penulis tidak melakukan implementasi peningkatan keamanan jaringan yang sudah ada namun hanya memberi solusi yang sebaiknya dilakukan untuk mengantisipasi terjadinya serangan.
3. Penulis hanya membatasi *hak akses user*, *firewall* dan *proxy*.
4. Sistem ini cowok dengan jaringan *wifi* rumah.
5. Penulis tidak membahas *manajemen bandwidth*.
6. Penulis tidak membahas *captive portal*.

#### 1.4 Tujuan Penelitian

Adapun tujuan dari penulis dalam penelitian ini adalah untuk menganalisa tingkat keamanan jaringan (*wifi*).

#### 1.5 Manfaat Penelitian

2. Manfaat yang diharapkan dari penelitian ini adalah untuk mengetahui tingkat keamanan pada Jaringan (*wifi*).
3. Sebagai pengetahuan bagi pengguna layanan/ fasilitas internet (*wifi*) khususnya bagi pengguna yang awam terhadap bahaya jaringan tanpa pengamanan.

#### 1.6 Metode Penelitian

Untuk mencapai hasil penelitian yang bagus penulis menggunakan metode:

##### 1.6.1 Metode SPDLC

Metode pengembangan system yang digunakan dalam penelitian ini adalah menggunakan pengembangan model SPDLC (*Security Policy Development Life Cycle*). Adapun terdiri dari 6 (enam) tahapan yaitu:

1. Tahapan Identifikasi
2. Tahapan Analisa
3. Tahapan Desain
4. Tahapan Implementasi
5. Tahapan Audit
6. Tahapan Evaluasi

## **1.7 Sistematika Penulisan**

Sistematika penulisan laporan ini disusun dalam beberapa bab sebagai berikut:

### **BAB I PENDAHULUAN**

Dalam bab ini berisi dan menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

### **BAB II LANDASAN TEORI**

Dalam bab ini berisi dasar-dasar teori yang digunakan dan mendukung dalam penelitian yang dilakukan.

### **BAB III ANALISIS DAN PERANCANGAN SISTEM**

Dalam bab ini berisi metode analisis pengumpulan data dan pengembangan sistem yang digunakan dalam proses penelitian.

### **BAB IV IMPLEMENTASI DAN PEMBAHASAN**

Dalam bab ini berisi analisis keamanan jaringan untuk mengetahui kelemahan dan memberikan solusi untuk memperbaiki kelemahan guna meningkatkan kualitas jaringan.

### **BAB V PENUTUP**

Dalam bab ini berisi kesimpulan yang dapat selama proses penelitian dan saran untuk pengembangan berikutnya.