

# BAB I PENDAHULUAN

## 1.1 Latar Belakang

Pada era digital saat ini, penggunaan jaringan internet menjadi sangat penting dan krusial dalam berbagai aspek kehidupan. Salah satu media komunikasi yang berkembang pesat adalah jaringan komunikasi internet berbasis *wireless*. *Wi-Fi* (*wireless fidelity*) merupakan teknologi komunikasi *wireless* yang memanfaatkan gelombang radio untuk menyediakan koneksi berkecepatan tinggi. Saat ini, *Wi-Fi* dapat dengan mudah dijumpai di berbagai tempat umum, seperti kafe, hotel, restoran, dan kantor pemerintahan. Kemudahan akses terhadap jaringan *wireless* membuat setiap orang dapat memanfaatkannya kapan saja [1].

Namun, meskipun penggunaan *Wi-Fi* semakin meluas, jaringan internet ini memiliki beberapa kelemahan, terutama dalam aspek keamanan. Contoh ancaman yang umum adalah serangan *hacker*, pencurian data informasi, dan serangan *Packet Sniffing*. Keamanan jaringan merupakan pelindung dalam sebuah sistem jaringan yang bertujuan untuk mencegah penggunaan oleh pihak yang tidak berhak dan tidak bertanggung jawab, serta untuk mengidentifikasi dan mencegah pengguna tidak sah (penyusup) dari mengakses jaringan computer [2].

Pada tanggal 12 April 2024 ada informasi dari pengelola bahwa, seorang tamu di penginapan La Tulip melaporkan menerima email *phishing* setelah menggunakan jaringan *Wi-Fi* penginapan saat mengakses sebuah *website*. Insiden ini menimbulkan kekhawatiran mengenai keamanan jaringan *Wi-Fi* publik di penginapan, terutama karena risiko bahwa jaringan tersebut dapat dimanfaatkan oleh penyerang untuk mencuri informasi sensitif dari tamu. Mengingat pentingnya perlindungan data pribadi dan keamanan komunikasi digital, perlu dilakukan penelitian untuk mengevaluasi tingkat keamanan jaringan *Wi-Fi* di penginapan La Tulip.

Penelitian ini bertujuan untuk memberikan pemahaman yang mendalam mengenai keamanan protokol *WPA* dan *WPA2* pada jaringan *Wi-Fi*, dengan fokus pada penginapan La Tulip. Hasil analisis dan rekomendasi yang dihasilkan diharapkan bermanfaat tidak hanya bagi pengelola penginapan La Tulip, tetapi juga bagi pengelola jaringan *Wi-Fi*. Penelitian ini berpotensi memberikan kontribusi signifikan dalam bidang keamanan jaringan nirkabel. Aplikasi yang akan digunakan dalam penelitian ini adalah *Ettercap* dan *Wireshark*. *Ettercap* akan digunakan untuk memverifikasi keamanan jaringan dan menganalisis protokol, serta mendengarkan protokol jaringan, mencuri kata sandi, dan memblokir lalu lintas. *Wireshark*, sebagai *network packet analyzer*, akan digunakan untuk mengumpulkan dan menampilkan data komunikasi jaringan secara detail[3].

## **1.2 Rumusan Masalah**

Berdasar latar belakang masalah yang telah dipaparkan sebelumnya, maka dapat disimpulkan masalah penelitian sebagai berikut:

1. Bagaimana tingkat keamanan *WPA* dan *WPA2* pada jaringan *Wi-Fi*?
2. Bagaimana efektivitas tools *Ettercap* dan *Wireshark* dalam menguji keamanan jaringan *Wi-Fi* yang menggunakan *WPA* dan *WPA2*?

## **1.3 Batasan Masalah**

Untuk mencegah meluasnya penelitian ini maka peneliti memberi Batasan pada permasalahan penelitian, diantaranya sebagai berikut:

1. Penelitian ini dibatasi pada analisis keamanan jaringan *Wi-Fi* yang menggunakan *WPA* dan *WPA2*.
2. Penelitian ini dibatasi pada penggunaan dua aplikasi utama, yaitu *Ettercap* dan *Wireshark*, untuk analisis dan verifikasi keamanan jaringan.
3. Data yang dikumpulkan dan dianalisis dalam penelitian ini terbatas pada hasil yang diperoleh dari penggunaan *Ettercap* dan *Wireshark*.

4. Penelitian ini dibatasi pada *Provider wifi* penginapan, yaitu Ringnet
5. Penelitian ini hanya dilakukan di Penginapan la tulip

#### 1.4 Tujuan Penelitian

Tujuan peneliti untuk menganalisis keamanan jaringan dari *WPA* dan *WPA2* diantaranya sebagai berikut:

1. Menilai Tingkat Keamanan *WPA* dan *WPA2* pada Jaringan *Wi-Fi*
2. Mengukur Efektivitas tools *Etercap* dan *Wireshark* dalam Menguji Keamanan Jaringan *Wi-Fi*
3. Memberikan Rekomendasi untuk Meningkatkan Keamanan Jaringan *Wi-Fi* di Penginapan La Tulip dan Tempat Lainnya

#### 1.5 Manfaat Penelitian

Adapun manfaat bagi peneliti yaitu :

1. Penelitian ini memberikan pemahaman yang lebih mendalam mengenai keamanan protokol *WPA* dan *WPA2*, sehingga pengelola jaringan dapat memahami risiko dan ancaman yang mungkin dihadapi.
2. Hasil analisis dari penelitian ini akan membantu mengidentifikasi potensi kelemahan dan ancaman pada protokol *WPA* dan *WPA2*, sehingga pengelola jaringan dapat mengambil tindakan pencegahan yang tepat.
3. Penelitian ini menunjukkan cara penggunaan aplikasi *Etercap* dan *Wireshark* untuk memverifikasi keamanan jaringan dan menganalisis protokol, sehingga dapat digunakan sebagai panduan bagi pengelola jaringan dalam melakukan pengujian keamanan.

## **1.6 Sistematika Penulisan**

### **BAB I : PENDAHULUAN**

Bab ini membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

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

Bab ini membahas tentang teori yang berupa kajian Pustaka yang mencakup penjelasan dari jurnal atau refrensi berhubungan dengan penelitian ini. Teori-teori tersebut diharapkan dapat dijadikan bahan pertimbangan dan pendukung penelitian.

### **BAB III : METODE PENELITIAN**

Bab ini membahas tentang metode penelitian yang digunakan, metode pengembangan jaringan berbasis NDLC (*Network Development Life Cycle*), metode analisis performa routing protocol, topologi yang akan digunakan, serta kebutuhan penelitian lainnya.

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

Bab ini membahas tentang rancangan penelitian yang mencakup langkah-langkah dan proses lengkap penelitian, serta implementasi serangan *sniffing* menggunakan *MitM attack* dan *ARP poisoning*. Pembahasan juga mencakup pengujian dan analisis hasil penelitian.

### **BAB V : KESIMPULAN DAN SARAN**

Bab ini berisikan kesimpulan dan saran dari penelitian yang telah dilakukan. Kesimpulan berisi pernyataan mengenai hasil dari penelitian dan saran berupa pendapat peneliti untuk penelitian yang akan datang.