BAB I

PENDAHULUAN

1.1 Latar belakang

Perkembangan teknologi informasi dan komunikasi yang begitu pesat telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam hal akses terhadap jaringan *internet*. Jaringan nirkabel (*WiFi*) telah menjadi solusi utama dalam penyediaan layanan konektivitas karena sifatnya yang fleksibel dan efisien. *WiFi* digunakan secara luas di lingkungan rumah, institusi pendidikan, perkantoran, hingga fasilitas umum. Namun demikian, di balik kemudahan tersebut, jaringan *WiFi* memiliki potensi kerentanan yang cukup tinggi terhadap berbagai bentuk ancaman keamanan. (Okario et al., 2023)

Perencanaan dan pemahaman yang mendalam terhadap sistem keamanan jaringan *wireless* sangat penting untuk menjamin perlindungan yang optimal terhadap aset dan sumber daya yang terdapat dalam jaringan tersebut(Adiguna & Widagdo, 2022)

Sifat jaringan nirkabel yang terbuka memungkinkan pihak tidak bertanggung jawab untuk melakukan berbagai jenis serangan, seperti *sniffing, spoofing, brute force attack*, maupun *man-in-the-middle attack*.(Setyawan & Amnur, 2022) Ancaman-ancaman tersebut dapat menyebabkan kebocoran informasi, pencurian data, bahkan pengambilalihan akses terhadap sistem. Kurangnya kesadaran pengguna dan lemahnya konfigurasi keamanan jaringan menjadi salah satu faktor utama yang menyebabkan tingginya tingkat kerentanan tersebut.

Permasalahan terkait keamanan jaringan juga dialami oleh PT *Evergrown Technology*, sebuah perusahaan yang memanfaatkan jaringan WiFi sebagai sarana utama untuk mendukung aktivitas operasional kantor. Dalam praktiknya, perusahaan menghadapi keluhan dari karyawan mengenai penurunan kecepatan internet yang semakin lama semakin buruk**,** yang disebabkan oleh banyaknya akses tidak sah pada jaringan WiFi perusahaan. Kondisi ini menunjukkan adanya celah keamanan yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab, sehingga berdampak pada efektivitas dan efisiensi kerja karyawan di lingkungan perusahaan.

Oleh karena itu, diperlukan upaya untuk melakukan analisis terhadap keamanan jaringan *WiFi* guna mengidentifikasi potensi celah keamanan yang ada. Salah satu pendekatan yang umum digunakan dalam melakukan pengujian terhadap keamanan jaringan adalah dengan memanfaatkan perangkat lunak *open source* seperti *Aircrack-ng*(Anam & Fachri, 2025). *Aircrack-ng* merupakan *tools* yang dirancang khusus untuk melakukan *audit* terhadap keamanan jaringan nirkabel, khususnya dalam menganalisis kelemahan pada sistem enkripsi *WEP* dan *WPA/WPA2*. Dalam implementasinya, *Aircrack-ng* dapat dijalankan secara optimal menggunakan sistem operasi *Kali Linux*, yang dikenal sebagai distribusi *Linux* yang ditujukan untuk keperluan *penetration testing* (Anam & Fachri, 2025) dan keamanan sistem informasi. Melalui kombinasi antara *Aircrack-ng* dan *Kali Linux*, dimungkinkan untuk melakukan simulasi serangan terhadap jaringan *WiFi* secara terstruktur dan bertanggung jawab, dengan tujuan utama untuk memperoleh

pemahaman yang lebih mendalam mengenai aspek-aspek keamanan jaringan nirkabel.

Berdasarkan latar belakang tersebut, penelitian ini dilakukan dengan tujuan untuk mengimplementasikan tools *Aircrack-ng* dalam menganalisis keamanan jaringan *WiFi* menggunakan sistem operasi *Kali Linux*. Diharapkan hasil dari penelitian ini dapat memberikan kontribusi dalam upaya peningkatan keamanan jaringan nirkabel serta menjadi referensi bagi pengguna dan pengelola jaringan dalam menerapkan langkah-langkah pengamanan yang tepat.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan, maka dapat diidentifikasi beberapa permasalahan sebagai berikut:

1. Jaringan *WiFi* rentan terhadap berbagai bentuk serangan siber seperti *sniffing*, *brute force*, dan *man-in-the-middle attack*, yang dapat membahayakan integritas dan kerahasiaan data.
2. Belum adanya upaya sistematis di PT *Evergrown Technology* dalam melakukan pengujian keamanan jaringan *WiFi* untuk mengetahui tingkat kerentanannya.
3. Diperlukan pemanfaatan *tools* khusus yang dapat digunakan untuk menganalisis dan mengidentifikasi celah keamanan pada jaringan *WiFi* secara efektif.

1.3 Rumusan Masalah

Berdasarkan latar belakang dan identifikasi masalah yang telah dijelaskan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana proses implementasi *tools Aircrack-ng* dalam menganalisis keamanan jaringan *WiFi*?
2. Sejauh mana efektivitas *Aircrack-ng* dalam mengidentifikasi celah keamanan pada jaringan *WiFi*?
3. Bagaimana melakukan mitigasi pada setiap fitur di perangkat *router wifi*?

1.4 Batasan masalah

Agar penelitian ini lebih terarah dan tidak melebar dari ruang lingkup yang telah ditentukan, maka penelitian dibatasi pada hal-hal berikut:

1. Penelitian ini hanya difokuskan pada analisis keamanan jaringan *WiFi* yang berada di lingkungan PT *Evergrown Technology*.
2. *Tools* yang digunakan dalam penelitian ini dibatasi pada penggunaan *Aircrack-ng* sebagai alat utama untuk melakukan *penetration testing* terhadap jaringan *WiFi*.
3. Sistem operasi yang digunakan dalam proses pengujian adalah *Kali Linux,* tanpa membandingkan dengan sistem operasi lainnya.
4. Pengujian hanya dilakukan terhadap jaringan WiFi internal yang telah mendapat izin dari pihak berwenang di PT *Evergrown Technology*, tanpa menyertakan jaringan eksternal atau publik.
5. Penelitian tidak mencakup perancangan sistem keamanan baru, melainkan hanya menganalisis tingkat keamanan dan memberikan rekomendasi berdasarkan hasil pengujian.

1.5 Tujuan Penelitian

Adapun tujuan dari penelitian ini yaitu ;

1. Untuk mengimplementasikan tools *Aircrack-ng* dalam melakukan analisis keamanan jaringan *WiFi* pada lingkungan PT *Evergrown Technology*.
2. Untuk mengetahui efektivitas *Aircrack-ng* dalam mengidentifikasi celah atau kelemahan pada sistem keamanan jaringan nirkabel.
3. Untuk melakukan mitigasi pada setiap fitur di perangkat router *wifi*.

1.6 Manfaat Penelitian

Penelitian ini memberikan kontribusi dalam dua aspek utama, yaitu manfaat teoritis dan manfaat praktis, sebagaimana dijabarkan berikut ini:

1. Manfaat Teoritis

   Penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan ilmu pengetahuan di bidang keamanan jaringan komputer, khususnya dalam konteks analisis kerentanan jaringan *WiFi* menggunakan *tools open-source*. Hasil penelitian ini dapat menjadi referensi akademik dalam studi keamanan jaringan dan penerapan metode *penetration testing* menggunakan sistem operasi berbasis *Linux*.

2. Manfaat Praktis

   Penelitian ini juga memiliki manfaat praktis bagi beberapa pihak terkait, antara lain:

a. Bagi Penulis:

   Penelitian ini memberikan pengalaman langsung dalam menerapkan tools keamanan jaringan secara nyata, meningkatkan pemahaman teknis, dan memperluas wawasan di bidang *ethical hacking* serta *network security*.

b. Bagi PT *Evergrown Technology*:

Penelitian ini dapat membantu perusahaan dalam mengidentifikasi celah keamanan pada jaringan *WiFi* yang digunakan, serta memberikan masukan dan rekomendasi perbaikan guna meningkatkan sistem keamanan informasi di lingkungan kerja.

c. Bagi Universitas Putera Batam:

   Hasil penelitian ini dapat menambah koleksi karya ilmiah yang relevan di bidang teknologi informasi dan keamanan jaringan, serta menjadi bahan referensi untuk pengembangan kurikulum atau kegiatan akademik lainnya.

d. Bagi Peneliti Selanjutnya:

   Penelitian ini dapat menjadi dasar atau acuan bagi penelitian-penelitian lanjutan yang ingin mengkaji topik serupa, baik dengan pendekatan yang lebih luas, penggunaan *tools* berbeda, maupun pengujian pada lingkungan jaringan yang lebih kompleks.