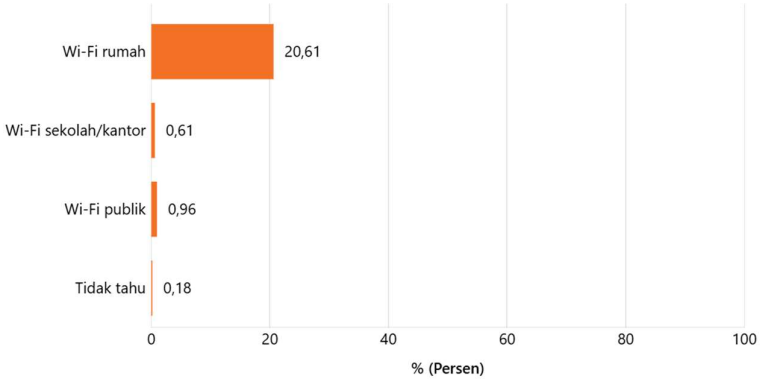
# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Modernisasi di bidang teknologi informasi, secara khusus terkait jaringan komputer, telah membawa perubahan signifikan dalam cara manusia bertukar informasi. Media transmisi data pada jaringan komputer terbagi menjadi dua kategori utama: sistem berkabel dan nirkabel. Pada sistem nirkabel, komunikasi antar perangkat dilakukan melalui gelombang radio, menghilangkan kebutuhan akan sambungan kabel fisik untuk menghubungkan satu perangkat dengan perangkat lainnya. [1]. Pada teknologi nirkabel, proses pengiriman data dilakukan menggunakan gelombang radio yang dipancarkan secara menyebar dan dapat merambat bebas melalui medium udara. Hal ini memungkinkan pengiriman informasi ke area yang dapat dijangkau oleh sinyal radio tersebut tanpa memerlukan kabel. Namun, media transmisi *Wireless* memiliki kelemahan dibandingkan dengan media kabel. Karena memanfaatkan gelombang radio untuk mentransmisikan data, sistem jaringan nirkabel menjadi lebih mudah terekspos terhadap berbagai bentuk serangan [2].

Berdasarkan data yang dirilis APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), penetrasi internet di Indonesia mengalami pertumbuhan, dengan total pengguna mencapai 215,63 juta orang pada periode 2022-2023. Angka ini menunjukkan kenaikan sebesar 2,67% dibandingkan tahun sebelumnya yang tercatat 210,03 juta pengguna. Dari total populasi Indonesia yang berjumlah 275,77 juta jiwa, pengguna internet telah mencakup 78,19% penduduk. [3]. Meski terjadi peningkatan kecepatan internet di Indonesia dari 17,37 Mbps di Maret 2021 ke 21,23 Mbps di Maret 2022, namun posisi Indonesia masih berada di bawah negara-negara tetangga di kawasan Asia Tenggara dalam hal performa internet. [4][5].




Gambar 1.1 Statistik jumlah pengguna Layanan *Wi-Fi*

APJII mengungkapkan penetrasi, dimana Pada Juni 2022, sebesar 22,13% pengguna internet di Indonesia mengakses internet melalui *Wi-Fi* [6]. Di era digital ini, aspek keamanan pada jaringan internet, khususnya yang menggunakan WLAN, menjadi faktor krusial yang membutuhkan perhatian serius. Hal ini dikarenakan setiap jaringan yang terkoneksi ke internet memiliki potensi kerentanan dan dapat menjadi target eksploitasi oleh peretas [7]. Sampai saat ini, jenis serangan yang umum terjadi pada jaringan *Wi-Fi* adalah Titik Akses Palsu (*Fake AP*) dan Serangan *Man in the Middle* [8].

Serangan *Man in the Middle* (MITM) menjadi ancaman signifikan dalam keamanan siber. Menurut sebuah studi pada 2021, Serangan MITM mewakili 19% dari seluruh serangan siber yang berhasil. Lebih lanjut, laporan F5 tahun 2022 mengungkapkan bahwa Lebih dari 50% serangan MITM melibatkan intersepsi informasi sensitif, termasuk kredensial *login* dan informasi perbankan [9]. *Man in the Middle* (MITM) adalah serangan keamanan komputer yang menargetkan koneksi HTTP antara pengguna dan *website*. Tujuannya adalah mencuri kerahasiaan dan mengkompromikan integritas aliran data antara *server* dan pengguna. Adapun *Evil Twin Attack* ini mencakup serangan Titik Akses Palsu (Fake AP) dan Serangan *Man in the Middle*, yang merupakan metode penyerangan jaringan *Wi-Fi* yang saling terkait untuk penyerang mendapatkan data pribadi seperti *password*.

*Evil Twin* merupakan jenis serangan jaringan yang memanfaatkan teknik *Man in the Middle* (MITM). Dalam serangan ini, penyerang menciptakan jaringan dengan SSID yang sama untuk menipu korban agar terhubung ke jaringan palsu dan diarahkan ke halaman *login* tiruan. *Evil Twin Fake* adalah salah satu metode yang digunakan oleh peretas untuk menyusup ke dalam jaringan dan mengumpulkan informasi milik korban (Information Harvesting). [10]. Ketika pengguna terhubung ke jaringan *Wi-Fi* palsu ini, hacker dapat dengan mudah mencegat data mereka, seperti *password*, informasi pribadi.

Oleh karena itu, analisis keamanan jaringan pada layanan *Wi-Fi* XL Home terhadap serangan *Evil Twin* menjadi penting untuk menganalisis keamanan jaringan *Wi-Fi* XL Home terhadap serangan *Evil Twin* dan memberikan rekomendasi untuk meningkatkan keamanan pada jaringan *Wi-Fi* XL Home. Analisis semacam ini mencakup pengujian *Quality of Service* (QoS) pada jaringan *Wi-Fi* XL Home dan Penyerang *Evil Twin* membuat jaringan *Wi-Fi* palsu dengan nama yang mirip dengan jaringan *Wi-Fi* XL Home yang sah. Serangan *Evil Twin*, yang bisa dilakukan dengan *tool* seperti *Airgeddon* di *Kali Linux*, dan penelitian ini juga bertujuan untuk memahami mengapa kejahatan siber terkait *Wi-Fi* marak terjadi, serta menganalisis cara kerja *Evil Twin* pada layanan *Wi-Fi* XL Home. Selain itu, penelitian ini juga bertujuan untuk meningkatkan kesadaran pengguna tentang bahaya serangan tersebut.

## 1.2 Perumusan Masalah

Dari Latar belakang di atas maka diperoleh rumusan masalah:keamanan jaringan *Wi-Fi* XL Home terhadap serangan *Evil Twin* antara lain :

1. Berdasarkan banyaknya penggunaan *Wi-Fi* dan risiko serangan siber pada jaringan *Wireless*, Belum diketahui mengapa serangan *Evil Twin* yang dapat dengan mudah mengambil informasi dari pengguna layanan *Wi-Fi*.

2. Dampak serangan *Deauthentication* terhadap Kualitas jaringan *Wi-Fi* melalui pengukuran *Quality of Service* (QoS) parameter *Delay*, *Packet loss*, *Throughput*, dan *Jitter*.

**1.3 Pertanyaan Penelitian**

Dari hasil penjelasan di atas, peneliti merumuskan pertanyaan-pertanyaan yang akan dibahas, yaitu:

1. Mengapa serangan *Evil Twin* dapat dengan mudah mengambil informasi dari pengguna layanan *Wi-Fi*, mengingat banyaknya penggunaan *Wi-Fi* dan meningkatnya risiko serangan siber pada jaringan *Wireless*?
2. Bagaimana dampak serangan *Deauthentication* terhadap kualitas jaringan *Wi-Fi*, berdasarkan pengukuran parameter *Quality of Service* (QoS) seperti *Delay*, *Packet loss*, *Throughput*, dan *Jitter*?

**1.4 Tujuan Penelitian**

Merujuk pada rumusan masalah yang ada, dapat diketahui bahwa tujuan dari penelitian ini yaitu:

1. Menganalisis serangan *Evil Twin* dalam mengambil informasi dari pengguna layanan *Wi-Fi*, seiring dengan meningkatnya penggunaan *Wi-Fi* dan risiko serangan siber pada jaringan *Wireless*.
2. Mengidentifikasi dan menganalisis dampak serangan *Deauthentication* terhadap kualitas jaringan *Wi-Fi* dengan mengukur parameter *Quality of Service* (QoS), yaitu *Delay*, *Packet loss*, *Throughput*, dan *Jitter*.

**1.5 Batasan Masalah**

Berdasarkan perumusan masalah, tujuan, dan manfaat penelitian, batasan masalah untuk Analisis *Network Security* Pada Layanan *Wi-Fi* XL Home Terhadap Serangan *Evil Twin* sebagai berikut:

1. Penelitian ini difokuskan pada analisis keamanan jaringan *Wi-Fi* XL Home terhadap serangan *Evil Twin*.

2. Penelitian ini tidak membahas jenis serangan siber lainnya pada jaringan *Wi-Fi*
3. Penelitian ini akan membatasi pengukuran dan evaluasi *Quality of Service* (QoS) pada layanan Jaringan *Wi-Fi* XL Home. penelitian juga dilakukan dengan mengakses 2 *website* untuk pengujian jaringan internet. yaitu *website YouTube*, *Google Docs*.
4. Penelitian ini juga tidak membahas implementasi solusi secara langsung pada jaringan *Wi-Fi* XL Home.

## 1.6 Manfaat Penelitian

Berdasarkan penjelasan tersebut, penelitian ini mempunyai manfaat diantaranya:

1. Penelitian ini memberikan wawasan kepada masyarakat mengenai dampak serangan berbahaya dari jaringan *Wi-Fi* yang dapat merusak sebuah sistem.
2. Penelitian ini memberikan tambahan pengetahuan bagi penulis dan memperoleh secara langsung di bidang keamanan jaringan dalam menganalisis keamanan jaringan *Wi-Fi* terhadap serangan *Evil Twin*.