DAFTAR ISTILAH

APJII	: Asosiasi Penyelenggara Jasa Internet Indonesia
BSSN	: Badan Siber dan Sandi Negara
Pusopskamsinas	: Pusat Operasi keamanan Siber Nasional
WLAN	: *Wired Local Area Network*
QoS	: *Quality of Service*
TIPHON	: *Telecommunications and Internet Protocol Harmonization Over Networks*
AP	: *Access Point*
Wi-Fi	: *Wireless Fidelity*
IP	: *Internet Protocol*
CIA	: *Confidentiality, Integrity,* dan *Availability*
Mbps	: *Megabytes per second*
Kbps	: *kilobit per second*
ms	: *millisecond*
Notasi ilmiah "E-08"	: Dikali sepuluh pangkat negatif delapan "10^-8"
MITM	: *Man in the Middle*
SSID	: *Service Set Identifier*
BSSID	: *Basic Service Set Identifier*
MAC	: *Media Access Control Address*
HTTP	: *Hyper Text Transfer Protocol*
OSI	: *Open Systems Interconnection*
DHCP	: *Dynamic Host Configuration Protocol*
TCP	: *Transmission Control Protocol*
CSV	: *Comma Separated Values / File Excel*
DNS	: *Domain Name System*
WPA	: *Wi-Fi Protected Access*
VPN	: *Virtual Private Network*

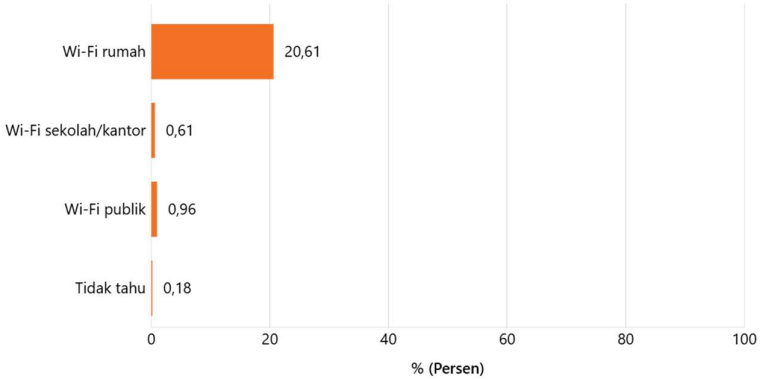
BAB I

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*.

BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Sebelumnya

Sebagai bagian dari penelitian yang akan dilakukan, Peneliti melakukan kajian literatur sebagai referensi dan saran untuk memperdalam pemahaman terhadap masalah yang diteliti sebagaimana tercantum dalam Tabel 2.1. Langkah ini dilakukan dengan tujuan penulis dapat memperoleh pemahaman yang lebih mendalam mengenai Analisis *Network Security* pada Layanan *Wi-Fi* XL Home terhadap serangan *Evil Twin*. Referensi ini adalah pekerjaan sebelumnya pada topik yang dibahas dan model yang digunakan. Berikut adalah beberapa penelitian sebelumnya tentang pertanyaan yang diajukan oleh para peneliti.

Penelitian "*EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled Wi-Fi*" Penelitian ini dilakukan oleh P. Shrivastava, M. S. Jamal, dan K. Kataoka. Jurnal ini berasal dari IEEE *Transactions on Network and Service Management*. Pada penelitian ini membahas masalah *Evil Twin Attack* menyerang dan mengkloning AP sah, menipu klien jaringan nirkabel untuk terhubung ke AP *Cloning* jahat. Berakibat pencurian data dan pemblokiran layanan. Berdasarkan hasil Penelitian ini telah melahirkan *EvilScout*, kerangka kerja yang dirancang untuk memerangi *Evil Twin Attack*. *EvilScout* memanfaatkan informasi distribusi awalan IP (*IP-prefix*) dari AP sah dan kekuatan SDN (*Software Defined Networking*) untuk mendeteksi *Evil Twin* dengan presisi tinggi dan hemat biaya [11].

Penelitian "*SLFAT: Client-Side Evil Twin Detection Approach Based on Arrival Time of Special Length Frames*" Penelitian ini dilakukan oleh Q. Lu, H. Qu, Y. Ouyang, and J. Zhang. Jurnal ini berasal dari *Security and Communication Networks*. Pada penelitian ini membahas masalah Keamanan jaringan *Wi-Fi* terancam oleh serangan *Evil Twin*. Penyerang dengan mudah

memalsukan identitas AP sah, menciptakan "*Evil Twin*" yang menipu pengguna untuk terhubung. Berdasarkan hasil Penelitian ini telah melahirkan *SLFAT (Speical Length Frames Arrival Time*), *SLFA* hadir sebagai solusi inovatif untuk memerangi *Evil Twin* di sisi klien. Pendekatan ini bekerja secara pasif dan ringan, tidak memerlukan perangkat khusus, dan dapat dijalankan pada perangkat nirkabel biasa [12].

Penelitian "*Network Security Analysis Simulation at the GCS in the UCAV to support the Indonesian Defense Area*" Penelitian ini dilakukan oleh B. Parga, None Anggi Zafia, and N. Iwan. Jurnal ini berasal dari Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi). Pada penelitian ini membahas Keamanan komunikasi data menjadi hal yang krusial dalam penerbangan UCAV jarak jauh. adanya Gangguan keamanan dapat menyebabkan terputusnya sinyal antara GCS (*Ground Control Station*) dan UCAV. Berdasarkan hasil Penelitian ini mengusulkan skema keamanan menggunakan *OpenVPN* di GCS untuk melindungi komunikasi UCAV. Kualitas Layanan QoS OpenVPN diuji dengan protokol ICMP, TCP, dan UDP untuk menentukan keandalan jaringan komunikasi UCAV. Hasil uji coba menunjukkan bahwa protokol ICMP memiliki tingkat kehilangan paket paling kecil (0%), protokol TCP memiliki tingkat kehilangan paket yang rendah (0.3%), dan protokol UDP memiliki *Delay* dan *Jitter* yang paling kecil (4.75 ms dan 0.22 ms) [13].

Penelitian "Implementasi Pengamanan Jaringan Dengan Teknik *Penetration Testing* Menggunakan Metode *Deauther* Dan *Evil Twin* Pada *Wireless* Tl - WR840N" Penelitian ini dilakukan oleh E. R. Mauluddin and T. Desyani. Jurnal ini berasal dari OKTAL : Jurnal Ilmu Komputer dan *Science*. Pada penelitian ini membahas Jaringan *Wi-Fi* yang tidak dienkripsi atau memiliki *password* lemah bagaikan gerbang terbuka bagi para peretas. Serangan seperti *Deauther* dan *Evil Twin* dapat dengan mudah menyusup ke jaringan *Wi-Fi*, mencuri data pribadi dan mengganggu komunikasi. Berdasarkan hasil dari Penelitian ini menunjukkan bahwa kedua metode ini

sangat efektif dalam meretas jaringan *Wi-Fi* yang tidak memiliki pengamanan yang memadai, seperti enkripsi lemah atau *password* yang mudah ditebak. Hal ini menjadi alarm bagi pengguna *Wi-Fi* untuk meningkatkan kewaspadaan dan memperkuat keamanan jaringan mereka [14].

Penelitian "Analisa dan Pengujian Serangan *Evil Twin* pada Jaringan berbasis *Wireless* dengan Keamanan WPA2-PSK" Penelitian ini dilakukan oleh R. Rinaldi and M. Sadikin. Jurnal ini berasal dari Ph. D. diss. Pada penelitian ini membahas Jaringan *Wi-Fi* dengan keamanan WPA2-PSK memiliki celah keamanan yang memungkinkan terjadinya serangan *Evil Twin*. Serangan ini dapat mencuri *password Wi-Fi* dan informasi pengguna, serta mengganggu koneksi *Wi-Fi* dan mengarahkan pengguna ke situs web berbahaya. Hal ini menimbulkan risiko keamanan yang signifikan bagi pengguna jaringan *Wi-Fi* dengan WPA2-PSK. Berdasarkan hasil dari Penelitian ini menunjukkan bahwa Penelitian ini menunjukkan bahwa serangan *Evil Twin* pada *Wi-Fi* dengan WPA2-PSK terbukti efektif dan dapat diatasi dengan meningkatkan keamanan jaringan menggunakan WPA2 *Enterprise* 802.1X *authentication*. Dengan menerapkan WPA2 *Enterprise* 802.1X *authentication*, jaringan *Wi-Fi* terlindungi dari serangan *Evil Twin* dan informasi pengguna terjamin keamanannya [10].

Penelitian "Evaluasi Peforma Jaringan Internet Menggunakan Metode QoS" Penelitian ini dilakukan oleh Aditya Dyan Ramadhan, Iwan Iskandar, Novriyanto,Pizaini. Jurnal ini berasal dari klik: Kajian Ilmiah Informatika dan Komputer. Pada penelitian ini membahas Melonjaknya penggunaan internet di SMK Labor Pekanbaru picu kekhawatiran penurunan kinerja jaringan. Akibatnya, kelancaran belajar mengajar terancam karena akses internet lambat dan koneksi tidak stabil. Berdasarkan hasil dari Penelitian ini mengukur kinerja jaringan internet di SMK Labor Pekanbaru menggunakan metode QoS. Parameter yang diukur meliputi *Throughput*, *Delay*, *Packet loss*, dan *Jitter*. Hasilnya menunjukkan bahwa kinerja jaringan bervariasi

tergantung waktu dan lokasi. Secara keseluruhan, kinerja jaringan tergolong baik dengan indeks QoS dan persentase 95-100% [15].

Penelitian "Analisis Kualitas Layanan Jaringan Internet *Wi-Fi* PT.XYZ dengan Metode QoS *(Quality of Service)*" Penelitian ini dilakukan oleh Muhammad Ryan Kamil, Fahmi Arzalega, Rosalinda, Asrul Sani. Jurnal ini berasal dari JBPI –Jurnal Bidang Penelitian Informatika. Pada penelitian ini Masalahnya terletak pada Jaringan internet tidak stabil di PT.XYZ (lambat, lag, hilang) mengganggu produktivitas karyawan. Peningkatan *bandwidth* atau perbaikan jaringan diperlukan untuk memastikan kelancaran kerja. Penelitian ini memiliki hasil pada Kinerja internet PT.XYZ tergantung ruang dan waktu. Throughput tertinggi tercatat di ruang pemasaran pada siang hari (9581 kbps) dan di ruang promosi pada sore hari (4520 kbps). Di sisi lain, packet loss tertinggi terjadi di ruang pemasaran pada pagi hari (3,5%) dan di ruang promosi pada sore hari (3,1%). Selain itu, delay dan jitter paling tinggi ditemukan di ruang pemasaran dan promosi saat siang hari (35,49 ms). Perlu optimasi jaringan untuk mengatasi ini [16].

Tabel 2.1 Ringkasan Penelitian Sebelumnya

No	Judul	Masalah	Hasil	Perbedaan
1.	*EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled Wi-Fi* (2020) [11]	Masalah *Evil Twin Attack* menyerang dan mengkloning AP sah, menipu klien jaringan nirkabel untuk terhubung ke AP *Cloning* jahat. Berakibat pencurian data dan pemblokiran layanan.	Berdasarkan hasil Penelitian ini telah melahirkan *EvilScout*, kerangka kerja yang dirancang untuk memerangi *Evil Twin Attack*. *EvilScout* memanfaatkan informasi distribusi awalan IP (*IP-prefix*) dari AP sah dan kekuatan SDN (*Software-Defined Networking*) untuk mendeteksi *Evil Twin* dengan presisi tinggi dan hemat biaya.	Perbedaan pada penelitian adalah Metodologi mengenai Mengimplementasikan kerangka kerja *EvilScout* pada *real* SDN *Wi-Fi* testbed dan mengevaluasi kinerjanya dalam mendeteksi *Evil Twin* sedangkan pada penelitian penulis Melakukan simulasi dan analisis teoritis untuk mengidentifikasi kerentanan dan mengusulkan solusi.
2.	*SLFAT: Client-Side Evil Twin Detection Approach Based on Arrival Time of Special Length Frames* (2019) [12]	Masalah Keamanan jaringan *Wi-Fi* terancam oleh serangan *Evil Twin*. Penyerang dengan mudah memalsukan identitas AP sah, menciptakan "*Evil Twin*" yang menipu pengguna untuk terhubung.	SLFAT hadir sebagai solusi inovatif untuk memerangi *Evil Twin* di sisi klien. Pendekatan ini bekerja secara pasif dan ringan, tidak memerlukan perangkat khusus, dan dapat dijalankan pada perangkat nirkabel biasa.	Perbedaan pada penelitian adalah pada penelitian sebelumnya menawarkan SLFAT sebagai solusi praktis untuk deteksi *Evil Twin* di sisi klien, sedangkan pada penelitian penulis memberikan wawasan tentang kerentanan keamanan spesifik pada jaringan *Wi-Fi* XL Home.
3.	*Network Security Analysis Simulation at*	Keamanan komunikasi data menjadi hal yang	Penelitian ini mengusulkan skema keamanan	Perbedaan pada penelitian adalah Penelitian ini

No	Judul	Masalah	Hasil	Perbedaan
	the GCS in the UCAV to support the Indonesian Defense Area (2022) [13]	krusial dalam penerbangan UCAV jarak jauh. adanya Gangguan keamanan dapat menyebabkan terputusnya sinyal antara GCS (*Ground Control Station*) dan UCAV.	menggunakan *OpenVPN* di GCS untuk melindungi komunikasi UCAV. Kualitas Layanan QoS OpenVPN diuji dengan protokol ICMP, TCP, dan UDP untuk menentukan keandalan jaringan komunikasi UCAV. Hasil uji coba menunjukkan bahwa protokol ICMP memiliki tingkat kehilangan paket paling kecil (0%), protokol TCP memiliki tingkat kehilangan paket yang rendah (0.3%), dan protokol UDP memiliki *Delay* dan *Jitter* yang paling kecil (4.75 ms dan 0.22 ms).	mengusulkan skema keamanan Berfokus pada analisis QoS OpenVPN di *Ground Control Station* (GCS) untuk mendukung komunikasi *Unmanned Combat Aerial Vehicle* (UCAV) dalam pertahanan Indonesia, sedangkan pada penelitian penulis analisis QoS pada layanan *Wi-Fi* XL Home untuk mengidentifikasi dampak serangan *Evil Twin*.
4.	Implementasi Pengamanan Jaringan Dengan Teknik *Penetration Testing* Menggunakan Metode *Deauther* Dan *Evil Twin* Pada *Wireless* Tl - WR840N (2024) [14]	Jaringan *Wi-Fi* yang tidak dienkripsi atau memiliki *password* lemah bagaikan gerbang terbuka bagi para peretas. Serangan seperti *Deauther* dan *Evil Twin* dapat dengan mudah menyusup ke jaringan *Wi-Fi*, mencuri data pribadi dan	Hasil dari Penelitian ini menunjukkan bahwa kedua metode ini sangat efektif dalam meretas jaringan *Wi-Fi* yang tidak memiliki pengamanan yang memadai, seperti enkripsi lemah atau *password* yang mudah ditebak. Hal ini menjadi alarm bagi pengguna *Wi-Fi* untuk meningkatkan	Perbedaan pada penelitian adalah metodologi penelitian sebelumnya mengimplementasi Pengamanan Jaringan menggunakan metode *Deauther* pada jaringan *Wi-Fi* Tl-WR840N sedangkan pada penelitian penulis Mengidentifikasi kerentanan keamanan pada jaringan *Wi-*

No	Judul	Masalah	Hasil	Perbedaan
		mengganggu komunikasi.	kewaspadaan dan memperkuat keamanan jaringan mereka.	*Fi* XL Home terhadap serangan *Evil Twin* saja.
5.	Analisa dan Pengujian Serangan *Evil Twin* pada Jaringan berbasis *Wireless* dengan Keamanan WPA2-PSK (2019) [10]	Jaringan *Wi-Fi* dengan keamanan WPA2-PSK memiliki celah keamanan yang memungkinkan terjadinya serangan *Evil Twin*. Serangan ini dapat mencuri *password Wi-Fi* dan informasi pengguna, serta mengganggu koneksi *Wi-Fi* dan mengarahkan pengguna ke situs web berbahaya. Hal ini menimbulkan risiko keamanan yang signifikan bagi pengguna jaringan *Wi-Fi* dengan WPA2-PSK.	Penelitian ini menunjukkan bahwa serangan *Evil Twin* pada *Wi-Fi* dengan WPA2-PSK terbukti efektif dan dapat diatasi dengan meningkatkan keamanan jaringan menggunakan WPA2 *Enterprise* 802.1X *authentication*. Dengan menerapkan WPA2 *Enterprise* 802.1X *authentication*, jaringan *Wi-Fi* terlindungi dari serangan *Evil Twin* dan informasi pengguna terjamin keamanannya.	Perbedaan penelitian sebelumnya adalah pada fokus penelitianya penelitian sebelumnya fokus pada analisis kerentanan WPA2-PSK terhadap *Evil Twin* dan mengusulkan solusi menggunakan WPA2 *Enterprise* dengan *RADIUS Server*. sedangkan pada penelitian penulis Berfokus pada identifikasi kerentanan *Evil Twin* pada layanan *Wi-Fi* XL Home dan memberikan rekomendasi mitigasi untuk ISP.
6.	Evaluasi Peforma Jaringan Internet Menggunakan Metode QoS (2023) [15]	Melonjaknya penggunaan internet di SMK Labor Pekanbaru picu kekhawatiran penurunan kinerja jaringan. Akibatnya, kelancaran belajar	Penelitian ini mengukur kinerja jaringan internet di SMK Labor Pekanbaru menggunakan metode QoS. Parameter yang diukur meliputi *Throughput*, *Delay*, *Packet loss*, dan *Jitter*. Hasilnya menunjukkan bahwa	Perbedaan penelitian sebelumnya terletak pada Temuan studi kasus yang dilakukan dalam penelitian sebelumnya. Pada penelitian sebelumnya, Kinerja jaringan di SMK Labor Pekanbaru

No	Judul	Masalah	Hasil	Perbedaan
		mengajar terancam karena akses internet lambat dan koneksi tidak stabil.	kinerja jaringan bervariasi tergantung waktu dan lokasi. Secara keseluruhan, kinerja jaringan tergolong baik dengan indeks QoS dan persentase 95-100%.	bervariasi tergantung waktu dan lokasi, dengan nilai QoS rata-rata tergolong baik. Namun, dalam penelitian penulis, temuan hasil analisis QoS hanya pada *Throughput*, *Delay*, dan *Packet loss*.
7.	Analisis Kualitas Layanan Jaringan Internet *Wi-Fi* PT.XYZ dengan Metode QoS *(Quality of Service)* (2023) [16]	Pada penelitian ini Masalahnya terletak pada Jaringan internet tidak stabil di PT.XYZ (lambat, lag, hilang) mengganggu produktivitas karyawan. Peningkatan bandwidth atau perbaikan jaringan diperlukan untuk memastikan kelancaran kerja.	Pada penelitian ini memiliki hasil pada Kinerja internet PT.XYZ fluktuatif tergantung ruang dan waktu. *Throughput* tertinggi di ruang pemasaran siang hari (9581 kbps) dan ruang promosi sore hari (4520 kbps). Namun, *Packet loss* tertinggi terukur di ruang pemasaran pagi hari (3,5%) dan ruang promosi sore hari (3,1%). Sementara itu, *Delay* dan *Jitter* tertinggi terjadi di ruang pemasaran dan promosi pada siang hari (35,49 ms). Perlu optimasi jaringan untuk mengatasi fluktuasi ini.	Perbedaan utama kedua penelitian ini terletak pada fokus dan metodenya. Penelitian sebelumnya berfokus pada pengukuran kinerja jaringan secara langsung, sedangkan penelitian penulis berfokus pada pengujian *Quality of Service* (QoS) pada jaringan *Wi-Fi* XL Home.

2.2 Landasan Teori

Landasan teori adalah pijakan ilmiah yang digunakan sebagai referensi dalam penelitian untuk memahami konsep-konsep utama yang relevan. Pada penelitian ini, teori-teori yang berkaitan dengan jaringan komputer, keamanan jaringan nirkabel, serangan *Evil Twin*, serta parameter *Quality of Service* (QoS) menjadi acuan utama.

2.2.1 Network Security

Keamanan Jaringan (*Network Security*) Keamanan jaringan komputer mencakup serangkaian praktik dan prosedur yang dirancang untuk melindungi jaringan dari ancaman dan serangan berbahaya, seperti virus, malware, peretas, dan pencurian data. Tujuan utamanya adalah menjaga kerahasiaan data sensitif serta mencegah kebocoran atau akses yang tidak diizinkan [17]. Terdapat lima prinsip utama yang harus diterapkan untuk menjaga keamanan jaringan, yaitu *Confidentiality, Integrity, Availability, Authentication, dan Access Control*. Tiga prinsip pertama dikenal sebagai CIA *Triad*, yang merupakan elemen dasar dalam keamanan jaringan. Untuk melengkapinya, diperlukan tambahan *Authentication* dan *Access Control* [18].

Gambar 2.1 CIA *Triad*.

Sumber: (CIA *Triad* Meaning: Confidentiality, Integrity, Availability (wallarm.com))