Terbit online pada laman web jurnal: **https://rjti.upp.ac.id/index.php/rjti**

RJTI
Riau Jurnal Teknik Informatika

Vol. 4 No. 2 (2025) 316 – 323| ISSN: 2829-2529 (Media Online)

Eksploitasi dan Pencegahan Serangan *Man In The Middle* (MITM) Dengan Teknik *Evil Twin* Pada Jaringan *Wi-Fi* Publik

Ulfiah Akhyasi[1], Ghufron Zaida Muflih[2]
[1,2]Teknik Informatika, Fakultas Teknik, Universitas Maarif Nahdlatul Ulama
[1]ulfiahokiyasi@gmail.com, [2]ghufron.zaida@umnu.ac.id

Abstract

Man In The Middle (MITM) attacks pose a serious threat to network security, especially on public Wi-Fi with low protection. One of the MITM methods commonly used is Evil Twin, namely creating an artificial access point that resembles a real network to trick users. This research aims to examine the implementation of Evil Twin attacks and efforts to prevent them. The approach used is experimental through simulations with software such as Aircrack-ng, Hostapd, and Wireshark for the sniffing process, as well as traffic monitoring using Zui. The simulation results show that the fake access point succeeded in trapping the victim's device for 10 minutes, and succeeded in intercepting more than 600 network activities, including 6 HTTP requests and 29 SSL sessions. Visualization via Zui indicates HTTP and SSL protocol spikes, as well as anomalous entries such as alert, weird, and capture_loss. As a mitigation measure, WiFi Analyzer is used to identify technical differences between fake and genuine access points, such as SSID, MAC address, channel and signal strength. This research confirms that attack simulation and early detection with simple tools can increase user awareness and awareness of MITM threats, while providing a practical approach that is easy to implement via smartphone devices.

Keywords: *Evil Twin, Man In The Middle, Wireshark, Wi-Fi Analyzer, Network Security, Public Wi-Fi.*

Abstrak

Serangan *Man In The Middle* (MITM) menjadi ancaman serius dalam keamanan jaringan, khususnya pada Wi-Fi publik dengan perlindungan rendah. Salah satu metode MITM yang umum digunakan adalah *Evil Twin*, yaitu pembuatan *access point* tiruan yang menyerupai jaringan asli untuk mengelabui pengguna. Penelitian ini bertujuan mengkaji pelaksanaan serangan *Evil Twin* serta upaya pencegahannya. Pendekatan yang digunakan bersifat eksperimental melalui simulasi dengan perangkat lunak seperti Aircrack-ng, Hostapd, dan Wireshark untuk proses *sniffing*, serta pemantauan lalu lintas menggunakan Zui. Hasil simulasi menunjukkan bahwa *access point* palsu berhasil menjebak perangkat korban selama 10 menit, dan berhasil menyadap lebih dari 600 aktivitas jaringan, termasuk 6 permintaan HTTP dan 29 sesi SSL. Visualisasi melalui Zui mengindikasikan lonjakan protokol HTTP dan SSL, serta entri anomali seperti *alert*, *weird*, dan *capture_loss*. Sebagai langkah mitigasi, *WiFi Analyzer* digunakan untuk mengenali perbedaan teknis antara *access point* palsu dan asli, seperti SSID, MAC address, channel, dan kekuatan sinyal. Penelitian ini menegaskan bahwa simulasi serangan dan deteksi awal dengan alat sederhana dapat meningkatkan kesadaran dan kewaspadaan pengguna terhadap ancaman MITM, sekaligus memberikan pendekatan praktis yang mudah diterapkan melalui perangkat smartphone.

Kata kunci: *Evil Twin, Man In The Middle, Wireshark, Wi-Fi Analyzer, Keamanan Jaringan, Wi-Fi Publik.*

1. Pendahuluan

Teknologi telah menjadi salah satu bagian yang tidak dapat dipisahkan dari kehidupan sehari-hari, baik dalam hal komunikasi, informasi, pendidikan, kesehatan, ekonomi, dan industri. Keterkaitan teknologi dengan berbagai aspek kehidupan telah memberikan banyak manfaat dan menjadikan cara kerja dunia lebih efisien. Selain itu, perkembangan teknologi juga telah membawa perubahan signifikan dalam berbagai sektor serta mempermudah akses informasi di seluruh dunia, [1]. Seiring dengan perkembangan teknologi juga telah memunculkan ancaman-ancaman yang dapat menyerang sisi keamanan dari teknologi tersebut khususnya di bidang teknologi jaringan [2], berdasarkan data dari laporan hasil monitoring keamanan siber nasional Badan Siber dan Sandi Negara (BSSN) untuk bulan desember 2024, mencatat sekitar 120.000 insiden serangan siber yang rata-rata 3.900-

4.200 kejadian perharinya, naik 10% dibandingkan November. Phishing menjadi kategori serangan terbanyak dengan 35% dari total insiden, diikuti malware sebesar 28%, *web defacement* 15%, *DDoS* 10%, dan serangan lain 12%. Dengan meningkatnya insiden phishing dan malware , ancaman terjadinya serangan *Man In The Middle* (MITM) melalui teknik *evil twin* semakin relevan maka dari itu diperlukannya keamanan siber untuk mengatasi masalah ini [3].

Dalam cakupannya keamanan siber terbagi menjadi beberapa jenis salah satunya yaitu keamanan jaringan atau *network security*. Keamanan jaringan merupakan sebuah proses atau teknologi yang dirancang untuk melindungi sistem komputer dari ancaman atau serangan yang dapat mencuri, merusak, serta mengubah informasi yang dikirim melalui jaringan sehingga komputer dapat terus beroperasi sebagaimana mestinya tanpa menghadapi hambatan apapun [4]. Di Indonesia, terdapat beragam jenis ancaman yang terus berkembang dan mengancam keamanan digital, seperti *malware, phishing, DDoS, MITM, cyberstalking,* identitas palsu, *cyberbullying*, kejahatan finansial dan serangan penelitian infrastruktur kritis [5], dari banyaknya jenis serangan *cyber* ini khususnya dalam ranah keamanan jaringan salah satunya melalui serangan *Man In The Middle.*

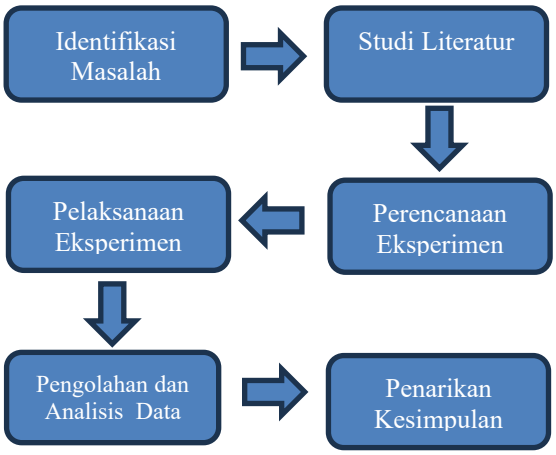
Serangan *Man In The Middle* merupakan salah satu jenis serangan dimana penyerang atau hacker menyusup kedalam interaksi antara dua pihak secara tersembunyi yang tidak disadari oleh kedua korban sehingga penyerang atau hacker dapat mengakses semua data yang melintas antara kedua pihak [6]. Dalam konteks jaringan publik seperti Wi-Fi gratis di tempat umum, serangan MITM kerap dilakukan menggunakan teknik *Evil Twin*, yaitu pembuatan *access point* palsu yang menyerupai jaringan asli. Teknik ini mengecoh pengguna agar terhubung ke jaringan tiruan sehingga penyerang dapat memantau lalu lintas data, terutama pada jaringan dengan enkripsi lemah seperti WEP atau WPA lama. Kurangnya kesadaran pengguna serta rendahnya penggunaan sistem deteksi dini membuat teknik ini sangat efektif. [7].

Penelitian ini bertujuan untuk mengevaluasi potensi serangan MITM dengan teknik *Evil Twin* melalui simulasi langsung di lingkungan nyata, serta mengkaji efektivitas pencegahannya menggunakan aplikasi Wi-Fi Analyzer dan visualisasi data menggunakan Zui. Kontribusi utama dari penelitian ini adalah memberikan pendekatan praktis berbasis alat terbuka untuk meningkatkan deteksi dini terhadap serangan jaringan, serta meningkatkan kesadaran keamanan pengguna terhadap ancaman di jaringan Wi-Fi publik. Simulasi dilakukan secara etis di lingkungan kost Bu Endah dengan izin resmi sebagai bagian dari kepatuhan terhadap etika penelitian. Penelitian ini menunjukan bahwa simulasi berbasis perangkat lunak terbuka dan aplikasi pendukung dapat memberikan pemahaman nyata terhadap celah keamanan jaringan serta solusi pencegahan yang praktis dan aplikatif. Saran untuk penelitian selanjutnya, uji coba dapat dilakukan pada jaringan dengan enkripsi WPA3 untuk mengevaluasi efektivitas teknik *Evil Twin* pada sistem yang lebih aman. Selain itu, integrasi sistem deteksi dini seperti *Wireless Intrusion Detection System* (WIDS) otomatis berbasis perangkat IoT atau machine learning juga dapat dikembangkan guna meningkatkan keamanan jaringan secara *real-time*.

2. Metode Penelitian

Metode eksperimental merupakan teknik penelitian yang bertujuan untuk menguji hubungan sebab-akibat antara variabel dengan cara memodifikasi variabel independen dan mengamati pengaruhnya terhadap variabel dependen [8]. Dalam konteks keamanan jaringan, pendekatan ini memungkinkan dilakukannya simulasi serangan, seperti Man-in-the-Middle (MITM) menggunakan teknik *Evil twin*, serta penerapan langkah pencegahan menggunakan aplikasi *Wi-fi Analyzer*, Meskipun bukan merupakan sistem WIDS yang lengkap, aplikasi seperti *Wi-Fi Analyzer* di smartphone dapat digunakan sebagai alat bantu awal untuk memantau lingkungan jaringan nirkabel. Dengan fitur seperti pemetaan kanal dan kekuatan sinyal, pengguna dapat mendeteksi kehadiran *access point* asing yang mencurigakan, sehingga mendukung langkah awal dalam pencegahan gangguan jaringan. Dengan demikian, pendekatan eksperimen menyediakan data empiris yang valid mengenai efektivitas langkah-langkah keamanan yang diuji. Tahapan penelitian seperti pada Gambar 1.

DOI : https://doi.org/10.30606/rjti.v4i2.3473



Gambar 1. Tahapan Penelitian

1. Identifikasi Masalah adalah tahapan pertama dimana peneliti mengidentifikasi ancaman keamanan jaringan, khususnya serangan MITM dengan teknik *evil twin* di jaringan wi-fi publik.
2. Studi Literatur adalah tahapan kedua setelah identifikasi masalah yang menjelaskan konsep dasar, alat yang digunakan dan hasil penelitian terdahulu yang relevan.
3. Perencanaan Eksperimen adalah tahapan ketiga untuk menyusun scenario serangan MITM dengan teknik *evil twin* di lingkungan kos Bu Endah.
4. Pelaksanaan Eksperimen adalah tahapan keempat yaitu melakukan simulasi serangan MITM dengan teknik *evil twin*.
5. Pengolahan dan Analisis Data adalah tahapan kelima untuk menganalisis data hasil *sniffing* dan menguji efektifitas alat deteksi jaringan *wi-fi analyzer*.
6. Penarikan Kesimpulan adalah tahapan terakhir yang menyimpulkan efektifitas visualisasi dan pencegahan yang telah diterapkan.

3. Hasil dan Pembahasan

1. Identifikasi Masalah

Pada tahap identifikasi masalah, peneliti mulai menganalisis fenomena yang terjadi di lapangan terkait keamanan jaringan, khususnya pada Wi-Fi publik. Saat ini, semakin banyak tempat umum seperti café, taman kota, atau fasilitas publik lainnya yang menyediakan akses internet gratis melalui Wi-Fi. Sayangnya, jaringan semacam ini sering kali tidak dilengkapi dengan sistem keamanan yang kuat, sehingga rentan terhadap serangan siber, termasuk serangan *Man In The Middle* (MITM) berbasis *Evil Twin*. Hasil dari pengamatan ini menunjukan bahwa masih banyak pengguna yang terhubung ke jaringan wi-fi publik tanpa menyadari resiko keamanan jaringannya yang disebabkan oleh minimnya pemahaman pengguna tentang keberadaan acces point palsu (*evil twin*) dan kurangnya penggunaan system deteksi seperti WIDS pada jaringan wi-fi publik.

2. Studi Literartur

Setelah melakukan identifikasi masalah, peneliti melakukan studi literatur yang bertujuan untuk memperkuan dasar teori dan pemahaman peneliti terhadap topik yang di angkat serta meninjau hasil-hasil penelitian terdahulu yang relevan.

a. Landasan Teori

1. *Cyber Security* dan Keamanan Jaringan.

Cyber security adalah upaya atau rangkaian aktifitas yang dirancang untuk melindungi system computer, jaringan dan data dari serangan siber [9]. Keamanan jaringan adalah bagian dari cyber *security* yang secara khusus berfokus pada perlindungan terhadap jaringan komputer, baik local (LAN) maupun internet (WAN) dari berbagai jenis ancaman dan penyusup [10].

2. Serangan MITM dan *Evil Twin*

Serangan MITM merupakan salah satu jenis serangan yang dimana penyerang atau hacker menyusup kedalam interaksi antara dua pihak secara tersembunyi yang tidak disadari oleh kedua korban sehingga hacker dapat mengakses semua data yang ditransmisikan [11]. Beberapa teknik serangan dapat dilakukan pada serangan MITM salah satunya *evil twin, evil twin* adalah teknik serangan dengan cara membuat titik acces palsu yang menyerupai jaringan yang dituju dengan tujuan agar korban tersambung ke dalam AP palsu tanpa disadari [12].

3. Brim Zui dan *Wifi Analyzer*

BRIM ZUI (*Basis Rekam Informasi Multimedia dengan Zooming User Interface*) merupakan sistem visual interaktif yang dirancang untuk menganalisis data digital kompleks dalam konteks penyidikan siber. Dengan memanfaatkan teknik zoom-in dan zoom-out, sistem ini memungkinkan penyidik menjelajahi data besar secara visual, sehingga hubungan antar entitas digital dapat dipahami lebih mudah dibandingkan penyajian dalam bentuk teks atau tabel konvensional [13]. *WiFi Analyzer* yang dikembangkan oleh Abdelrahman M. Sid merupakan aplikasi berbasis Android yang berfungsi sebagai alat bantu dalam proses analisis dan optimasi jaringan nirkabel (WiFi). Aplikasi ini menyediakan berbagai fitur yang memungkinkan pengguna untuk memantau parameter teknis jaringan, seperti identitas SSID, kekuatan sinyal

DOI : https://doi.org/10.30606/rjti.v4i2.3473

(RSSI), frekuensi operasi (2,4 GHz, 5 GHz, hingga 6 GHz), serta informasi kanal yang digunakan oleh access point (AP) di sekitar [14].

b. Penelitian Terdahulu

Beberapa penelitian sebelumnya menjadi acuan dalam merancang pendekatan penelitian ini, terutama yang menguji serangan MITM dengan berbagai tools seperti Basori et al. (2024) dengan judul MITM smenggunakan Ettercap, lalu Auliafitria et al. (2024) dengan judul MITM dengan websploit, dan Fuad (2022) dengan judul MITM open-source dengan Bettercap. Berdasarkan hasi kajian tersebut menunjukan bahwa Sebagian besar penelitian hanya menekankan pada serangan, tanpa menampilkan visalisasi data secara *real-time* atau mengomninasikannya dengan system deteksi seperti WIDS.

3. Perencanaan Eksperimen

Pada perencanaan eksperimen dilakukan persiapan untuk pelaksanaan eksperimen seperti tempat pelaksaan yang akan dilakukan di café teman hati kebumen , alat atau perangkat yang dibutuhkan, dan sekenario serangan sebagai berikut:

Berikut alat yang dibutuhkan, seperti pada table 1.

Tabel 1. Alat dan Bahan Penelitian

Nama Alat	Deskripsi
Laptop	Lenovo IdeaPad 314ADA05, Processor AMD 3020e with Raden Graphics,RAM 8,00 GB, Sistem Operasi Windows 11
Adaptor Wi-Fi	TP-Link TL-WN722N Version 1 (Chipset : Atheros AR9271) dan TP-Link TL-WN722N Version 2/3
Linux	Sistem operasi yang digunakan
Aircrack-ng/airmon-ng	Memutus koneksi korban dari AP asli ke AP palsu
Hostapd	Membuat titik akses palsu atau *evil twin*
Dnsmasq	Mengonfigurasi DHCP dan DNS pada jaringan palsu
Iptables	Melakukan Nat dan menjembatani koneksi internet korban
Ettercap/mitm proxy	Melakukan serangan MITM, sniffing, injection
Wireshark/tcp dump	Monitor dan analisis lalu lintas data korban
Systemctl/nmcli	Mengontrol Koneksi Korban
Hp Oppo A54	Sebagai Korban
Wifi Analyzer	Mendeteksi access point mencurigakan

Berikut scenario simulasi serangan yang akan di lakukan,

1. Menyiapkan perangkat dengan sistem operasi Linux yang dilengkapi dengan perangkat lunak yang dibutuhkan, seperti *Aircrack-ng, Hostapd, Dnsmasq, Wireshark, Ettercap Wi-Fi, dan SSLstrip.*
2. Membuat titik akses palsu yang meniru jaringan Wi-Fi publik yang ada, dalam hal ini menggunakan jaringan Wi-Fi BUNDA KOST 2 dan membuat titik akses palsu dengan nama BUNDA KOST 3.
3. Penyerang menghubungkan perangkat yang sudah disiapkan dengan jaringan Wi-Fi publik yang ditargetkan, dan kemudian menjebak perangkat korban untuk terhubung ke jaringan palsu yang telah dibuat.
4. Pemantauan dan analisis data menggunakan wireshark
5. Visualisai data menggunakan ELK Stack dalam bentuk diagram batang
6. Menerapkan Wifi Analyzer untuk mendeteksi AP palsu untuk pencegahan serangan.

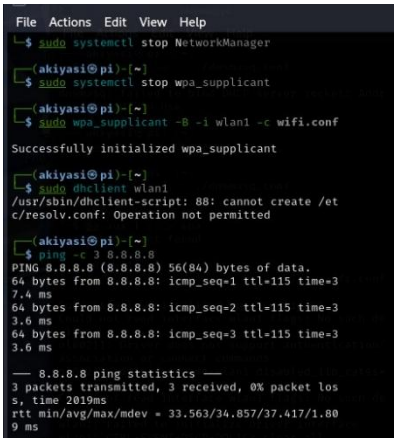
4. Pelaksanaan Eksperimen

Sebelum melakukan simulasi, lakukan instalasi semua tools dan paket yang diperlukan yaitu airmon-ng, hostapd, dnsmasq, iptables, Ettercap, wireshark, systemctl, ELK stack, Wifi Analyzer.

a. Simulasi Serangan MITM Teknik evil twin

1. Terminal 1 menyambungkan koneksi internet seperti pada gambar 2.

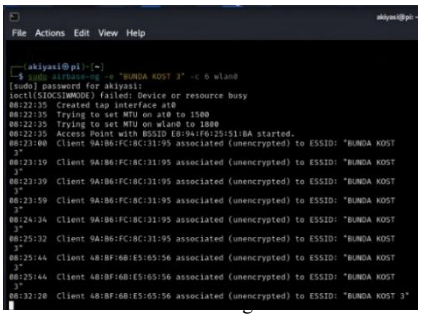
DOI : https://doi.org/10.30606/rjti.v4i2.3473



Gambar 2. Sniffing terminal 1

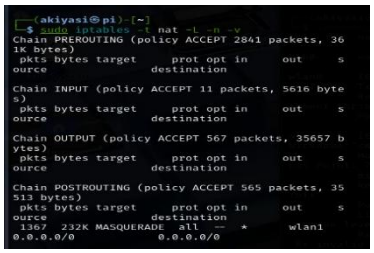
Langkah pertama adalah menghubungkan salah satu antarmuka jaringan wlan1 yang menggunakan adaptor TP-Link TL-WN722N versi 2/3 ke jaringan internet. Hal ini penting agar perangkat target yang terkoneksi ke jaringan palsu (Evil Twin) tetap mendapatkan akses ke internet—sehingga pengguna tidak mencurigai adanya manipulasi jaringan dengan mematikan layanan NetworkManager dan wpa_supplicant untuk mencegah konflik selama proses penyambungan jaringan secara manual. Setelah itu, wpa_supplicant dijalankan dengan antarmuka wlan1 menggunakan file konfigurasi wifi.conf, yang berisi informasi koneksi ke jaringan Wi-Fi asli. Ketika proses berhasil, muncul keluaran berupa pesan "successfully initialized wpa_supplicant" yang menandakan bahwa koneksi sudah tersambung. Selanjutnya, perintah dhclient dijalankan untuk mendapatkan IP address dari DHCP server jaringan asli, dan mengecek apakah sudah ada internet yang tersambung di titik akses palsu tersebut dengan kode ping -c 3.8.8.8.8.

2. Terminal 2 Untuk Menjalankan *Acces Point* Palsu (Evil Twin) seperti pada gambar 3.



Di terminal kedua, digunakan alat airbase-ng untuk membuat access point palsu dengan SSID "BUNDA KOST 3", yaitu nama yang mirip dengan jaringan WiFi asli, agar terlihat identik oleh perangkat korban. Access point dijalankan di antarmuka wlan0 menggunakan adaptor TP-Link TL-WN722N versi 1 dengan chipset Atheros yang mendukung fitur acces point dan disetel pada channel 6. Dengan begitu, perangkat yang mencari jaringan WiFi tersebut akan dengan mudah terkoneksi ke jaringan palsu yang sudah disiapkan oleh penyerang, pada terminal ini juga akan terlihat ip korban yang tersambung ke jaringan tersebut.

3. Terminal 3 untuk Konfigurasi IP dan Routing seperti pada gambar 4.



Gambar 4. Sniffing teminal 3

Setelah *access point* aktif, terminal ketiga digunakan untuk mengatur jalur lalu lintas data. Pertama-tama, antarmuka virtual at0 (hasil dari airbase-ng) diberikan IP address secara manual dengan subnet yang sesuai. Selanjutnya, proses IP forwarding diaktifkan agar sistem dapat meneruskan paket data dari korban ke internet melalui wlan1. Untuk mendukung fungsi ini, konfigurasi NAT dilakukan menggunakan iptables, yaitu dengan menghapus aturan lama dan menambahkan aturan baru yang mengatur agar semua lalu lintas dari interface at0 diarahkan ke wlan1 dan sebaliknya. Selain itu, parameter kernel net.ipv4.ip_forward juga diatur agar bernilai 1 sebagai tanda bahwa sistem telah siap meneruskan lalu lintas data. Perintah terakhir digunakan untuk memastikan semua aturan NAT sudah aktif dan siap digunakan.

4. Sniffing (Penyadapan Data Menggunakan Wireshark) seperti pada gambar 5.

Gambar 5. Sniffing wireshark

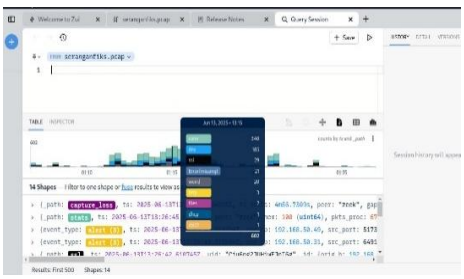
Untuk melakukan monitor dan penyadapan data secara real-time menggunakan Wireshark, aplikasi ini dijalankan dengan akses superuser dan diarahkan untuk memantau antarmuka at0, yaitu jalur komunikasi antara korban dan gateway. Dengan posisi ini, penyerang dapat menangkap berbagai jenis paket data yang dikirim atau diterima oleh perangkat korban, termasuk permintaan HTTP, login form, maupun data sensitif lainnya. Semua lalu lintas ini direkam untuk dianalisis lebih lanjut sebagai bagian dari evaluasi efektivitas

DOI : https://doi.org/10.30606/rjti.v4i2.3473

serangan dan potensi risiko keamanan. Pada gambar dibawah ini penyerang telah berhasil membangun dan mengoperasikan access point Evil Twin (seperti yang ditunjukkan oleh penangkapan data dari antarmuka at0), dapat secara efektif memantau dan menyadap seluruh komunikasi data yang melewati jaringan palsu tersebut dari perangkat korban. Secara spesifik, keberadaan lalu lintas HTTP yang tidak terenkripsi (terlihat dari 208 GET /connecttest.txt HTTP/1.1) menyoroti kerentanan serius, karena data tersebut dapat diakses dan dibaca langsung oleh penyerang, membuka peluang untuk pencurian informasi sensitif seperti kredensial. Meskipun ada juga lalu lintas yang menggunakan protokol terenkripsi seperti TLSv1.3, adanya lalu lintas HTTP yang terekspos tetap menjadi bukti nyata celah keamanan yang signifikan. Oleh karena itu, bukti visual dari sniffing ini sangat mendukung argumen mengenai pentingnya langkah-langkah pencegahan, seperti penggunaan *Virtual Private Network* (VPN) dan selalu memastikan koneksi HTTPS, untuk melindungi data pengguna saat terhubung ke jaringan Wi-Fi publik yang rentan terhadap serangan *Evil Twin*.

Selama simulasi berlangsung, durasi serangan yang berhasil direkam menggunakan *Wireshark* adalah sekitar 10 menit, dimulai pada pukul 13:15 hingga 13:25 waktu sistem. Dalam rentang waktu tersebut, perangkat korban secara aktif terhubung ke *access point* palsu dan mengirimkan lalu lintas data melalui jaringan yang telah dimanipulasi. Berdasarkan hasil visualisasi file seranganfiks.pcap di Zui, tercatat total 602 aktivitas jaringan pada puncak trafik, yang terdiri dari 340 koneksi aktif (conn), 185 permintaan DNS, 29 sesi SSL, dan 6 permintaan HTTP yang tidak terenkripsi. Selain itu, terdapat 3 peringatan keamanan (alert) dan 20 aktivitas anomali (weird) yang mengindikasikan lalu lintas tidak normal. Temuan capture_loss yang terjadi selama 4 menit 56 detik memperkuat bukti bahwa terjadi interferensi atau kehilangan paket selama proses intersepsi data oleh *access point* palsu. Dengan demikian, data kuantitatif ini memberikan gambaran konkret tentang intensitas dan keberhasilan serangan MITM yang dilakukan.

b. Visualisasi Data Menggunakan Zui seperti pada gambar 6.



Gambar 6. Visualisasi Data

Dalam tampilan utama Zui, grafik batang memperlihatkan aktivitas jaringan berdasarkan waktu, dengan warna-warna berbeda yang merepresentasikan berbagai jenis protokol seperti ssl, http, dns, conn, hingga alert. Terjadi lonjakan aktivitas pada beberapa titik waktu tertentu, yang mengindikasikan adanya anomali dalam jaringan. Salah satu temuan signifikan adalah tingginya jumlah koneksi ssl dan http, yang diduga kuat merupakan hasil dari pengguna yang secara tidak sadar terhubung ke *access point* palsu buatan penyerang. Aktivitas ini mencerminkan tujuan utama dari teknik Evil Twin, yaitu mendorong korban untuk menggunakan jaringan tiruan sehingga lalu lintas mereka dapat disadap oleh pelaku. Selain itu, ditemukan adanya entri yang mencurigakan pada alamat IP internal 192.168.50.15 yang muncul secara konsisten, menunjukkan sebagai sumber access point palsu atau perangkat penyerang.

Zui juga mencatat beberapa event abnormal seperti alert, weird, dan capture_loss, yang menunjukkan adanya gangguan atau anomali selama proses pengambilan data. Kehadiran capture_loss dalam jumlah besar dapat menjadi indikator terjadinya sniffing atau kehilangan paket karena interferensi, yang sering kali muncul pada skenario serangan Evil Twin. Selain itu, jenis lalu lintas yang terekam juga cukup bervariasi, dengan dominasi conn, dns, ssl, dan file x509, yang memperkuat bukti adanya manipulasi atau penyadapan lalu lintas jaringan yang menggunakan sertifikat palsu.

c. Penerapan *Wi-fi Analyzer* sebagai pencegahan seperti pada gambar 7.

Gambar 7. Wi-fi Analyzer

Hasil dari pemindaian dengan aplikasi WiFi Analyzer, terdeteksi dua access point dengan nama SSID yang mirip, yaitu BUNDA KOST 2 dan BUNDA KOST 3. Setelah dianalisis, BUNDA KOST 3 terindikasi sebagai Evil Twin. Hal ini terlihat dari beberapa perbedaan penting, seperti MAC address yang berbeda, channel yang tidak sama (CH 1 vs CH 6), serta kekuatan sinyal BUNDA KOST 3 yang jauh lebih tinggi (-16 dBm), menandakan perangkat tersebut sangat dekat dan kemungkinan sengaja dibuat agar menarik perhatian pengguna. Selain itu, BUNDA KOST 3 hanya menampilkan label keamanan [ESS] tanpa rincian

DOI : https://doi.org/10.30606/rjti.v4i2.3473

enkripsi, berbeda dengan BUNDA KOST 2 yang sudah menggunakan WPA-PSK-CCMP. Kombinasi faktor-faktor ini menunjukkan bahwa BUNDA KOST 3 adalah access point palsu yang dibuat untuk mengecoh pengguna dan membuka celah untuk serangan Man-in-the-Middle (MITM).

Dari sisi pencegahan, penggunaan aplikasi WiFi Analyzer menunjukkan hasil yang cukup responsif. Setelah jaringan dinyalakan, aplikasi membutuhkan waktu sekitar 10 detik untuk memindai dan menampilkan daftar SSID di sekitarnya. Dalam simulasi ini, dua SSID dengan nama mirip "BUNDA KOST 2" dan "BUNDA KOST 3" terdeteksi, namun yang terakhir teridentifikasi sebagai access point palsu berdasarkan perbedaan MAC address, channel (CH 1 vs CH 6), serta kekuatan sinyal yang mencolok (-16 dBm dibanding -43 dBm pada jaringan asli).

Salah satu keunggulan utama dari solusi yang diusulkan dalam penelitian ini adalah kepraktisannya. Aplikasi *WiFi Analyzer* dapat diunduh dan dijalankan langsung dari perangkat ponsel Android, tanpa memerlukan perangkat keras tambahan atau konfigurasi teknis yang kompleks. Hal ini memungkinkan pengguna awam sekalipun untuk melakukan deteksi mandiri terhadap keberadaan *access point* palsu secara cepat dan real-time. Dengan antarmuka yang sederhana dan visualisasi parameter seperti SSID, kekuatan sinyal, *channel*, dan tipe enkripsi, pengguna dapat mengidentifikasi jaringan yang mencurigakan dalam hitungan detik. Kepraktisan ini menjadikan Wi-fi Analyzer sebagai solusi awal yang sangat aplikatif, terutama bagi pengguna jaringan publik seperti di café, kampus, atau tempat umum lainnya, yang umumnya tidak memiliki perlindungan sistem jaringan yang canggih.

Meskipun aplikasi ini efektif dalam mengidentifikasi jaringan mencurigakan pada lingkungan terbatas, perlu dicatat bahwa WiFi Analyzer masih memiliki potensi gagal deteksi, terutama jika penyerang menggunakan metode spoofing yang meniru konfigurasi jaringan asli secara identik. Oleh karena itu, dalam kondisi dunia nyata yang lebih kompleks, penggunaan aplikasi ini sebaiknya dikombinasikan dengan sistem pemantauan jaringan lain seperti WIDS untuk meningkatkan akurasi dan keandalan deteksi.

5. Pengolahan dan Analisis Data

Data dalam penelitian ini diolah melalui tahapan simulasi serangan *Evil Twin* menggunakan berbagai tools, seperti Aircrack-ng, Hostapd, Dnsmasq, Wireshark, dan ELK Stack. Hasil dari simulasi ini mencakup lalu lintas jaringan, identifikasi *access point* tiruan, serta representasi visual dari aktivitas protokol yang berlangsung. Cuplikan data dari Wireshark mengungkap bahwa perangkat korban aktif bertukar data HTTP tanpa enkripsi ketika terhubung ke access point palsu bernama "BUNDA KOST 3", yang dibuat menyerupai SSID asli "BUNDA KOST 2". Permintaan HTTP seperti GET /connecttest.txt HTTP/1.1 menunjukkan bahwa serangan berhasil mengalihkan koneksi korban ke jaringan berbahaya. Data yang diperoleh kemudian diolah menggunakan Zui untuk melihat aktivitas jaringan secara real-time. Grafik batang menunjukkan lonjakan aktivitas pada protokol HTTP dan SSL, menandakan adanya koneksi dari korban ke access point palsu. Ditemukan pula IP mencurigakan 192.168.50.15, yang berperan sebagai sumber akses palsu. Selain itu, entri abnormal seperti alert, weird, dan capture_loss juga muncul selama proses pengumpulan data, menguatkan indikasi aktivitas berbahaya di jaringan. Access point palsu "BUNDA KOST 3" teridentifikasi melalui *WiFi Analyzer* berdasarkan perbedaan MAC address, channel, kekuatan sinyal, dan minimnya enkripsi. Serangan *Evil Twin* terbukti berhasil menjebak korban dan memungkinkan penyadapan data, sehingga menegaskan urgensi penerapan langkah mitigasi jaringan.

4. Kesimpulan

Berdasarkan hasil eksperimen yang telah dilakukan, dapat disimpulkan:

1. Teknik Evil Twin terbukti efektif untuk melakukan serangan MITM pada jaringan wi-fi publik yang tidak aman, terutama jika pengguna tidak waspada terhadap SSID yang mirip atau sama.
2. Wireshark dan Zui berhasil menangkap dan memvisualisasikan aktivitas jaringan secara *real-time*, menunjukan anomali lalu lintas yang di akibatkan oleh koneksi ke *access point* palsu.
3. Penggunaan aplikasi *WI-fi Analyzer* efektif sebagai alat deteksi awal terhadap keberadaan acces point palsu berdasarkan perbedaan teknis (MAC, channel,kekuatan sinyal, dan enkripsi)
4. Kesadaran pengguna sangat penting dalam mencegah serangan MITM dalam menghindari jaringan publik yang tidak terenkripsi, serta perhatian terhadap SSID yang mencurigakan dapat mengurangi resiko serangan secara signifikan.

Meskipun simulasi ini memberikan gambaran nyata tentang kerentanan jaringan publik terhadap serangan Evil Twin, penelitian ini memiliki beberapa keterbatasan. Salah satunya adalah kemampuan deteksi *Wi-Fi Analyzer* yang masih bergantung pada perbedaan teknis yang tampak, sehingga berpotensi gagal mendeteksi AP palsu jika penyerang meniru konfigurasi asli secara identik. Selain itu, simulasi dilakukan dalam lingkungan terbatas, yang belum tentu mewakili kondisi jaringan publik yang padat dan kompleks.

DOI : https://doi.org/10.30606/rjti.v4i2.3473

Oleh karena itu, penelitian lanjutan disarankan untuk menguji efektivitas deteksi pada jaringan dengan enkripsi modern seperti WPA3, serta mengeksplorasi penggunaan sistem deteksi intrusi nirkabel (WIDS) otomatis atau berbasis machine learning untuk meningkatkan perlindungan secara adaptif dan real-time.

Daftar Rujukan

[1] Fahmi *et al.*, *Perkembangan teknologi digitaluntuk berbagai bidang kehidupan (digital teknologi for humanity)*. Medan: USU Press, 2024. [Online]. Available: usupress.usu.ac.id

[2] G. zaida Muflih, S. Sunardi, I. Riadi, A. Yudhana, and himawan i Azmi, "Comparison of Forensic Tools on Social Media Services Using the Digital Forensic Research Workshop Method (DFRWS)," *JIKO*, vol. 1, 2023.

[3] Badan Sandi dan Siber Negara, "Laporan Bulanan Publik Mei 2024," depok, 2024. [Online]. Available: www.idsirtii.or.id

[4] K. Aziz, S. Zakir, W. Aprison, and L. Efriyanti, "Implementasi Keamanan Jaringan Dengan Metode Firewall Filtering Menggunakan Mikrotik Di SMK Payakumbuh," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 3, pp. 3343–3352, May 2024, doi: 10.36040/jati.v8i3.9662.

[5] R. D. Hapsari and K. G. Pambayun, "Ancaman Cybercrime di Indonesia," *J. Konstituen*, vol. 5, no. 1, pp. 1–17, Oct. 2023, doi: 10.33701/jk.v5i1.3208.

[6] I. Riadi, R. Umar, and I. Busthomi, "Optimasi Keamanan Autentikasi dari Man in the Middle Attack (MiTM) Menggunakan Teknologi Blockchain," *J. Inf. Eng. Educ. Technol.*, vol. 4, no. 1, pp. 15–19, Jun. 2020, doi: 10.26740/jieet.v4n1.p15-19.

[7] M. N. Hafizh, I. Riadi, and A. Fadlil, "Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic," *J. Telekomun. dan Komput.*, vol. 10, no. 2, p. 111, Aug. 2020, doi: 10.22441/incomtech.v10i2.8757.

[8] B. Sudaryana and R. Agusiady, *Metode Penelitian Kuantitatif*. Yogyakarta: Deeppublish Publisher, 2022.

[9] M. Gitlin and M. j. Goldstein, *Cyber Attack*. Twenty-First Century Books, 2015.

[10] Nirsal *et al.*, *Pengantar Jaringan dan Internet*. Jambi: PT.Senopati Publishing Indonesia, 2023.

[11] W. Seneru *et al.*, *Pengantar Teknologi Informasi dan Komunikasi*. Batam: Yayasan Cendikia Mulia Mandiri, 2025.

[12] A. E. Syaputra *et al.*, *Keamanan Jaringan Komputer*. Banten: PT Sada Kurnia Pustaka, 2025.

[13] D. Weissman and A. P. Jayasumana, "Lightweight Dataset for Decoy Development to Improve IoT Security," in *Computer Science, Engineering and Information Technology*, Academy & Industry Research Collaboration Center, Jul. 2024, pp. 127–140. doi: 10.5121/csit.2024.141410.

[14] Y. S. Belutowe, "Analysis Of 2.4GHz.and 5GHz Frequency Channels in Hostpot Area Distribution," vol. 8, no. 4, pp. 1009–1021, 2024, doi: 10.52362/jisamar.v8i4.1655.

DOI : https://doi.org/10.30606/rjti.v4i2.3473