e-ISSN 2549-7472
Edumatic: Jurnal Pendidikan Informatika
Vol. 9 No. 2, Agustus, 2025, **Hal. 629-638**
DOI: 10.29408/edumatic.v9i2.31822

Studi Eksperimen Keamanan Jaringan Wi-Fi Kampus: Analisis Kerentanan terhadap Serangan Evil Twin dan Deauthentication

Kia Putri Asiana [1,*], Raphael Bianco Huwae [1], Andy Hidayat Jatmika [1]

[1] Program Studi Teknik Informatika, Universitas Mataram, Indonesia
[*] Correspondence: kiaputriasiana@gmail.com

Copyright: © 2025 by the authors

Received: 26 Juli 2025 | Revised: 9 Agustus 2025 | Accepted: 20 Agusutus 2025 | Published: 23 Agustus 2025

Abstrak
Penggunaan Wi-Fi di perguruan tinggi semakin meningkat, namun disertai risiko keamanan seperti *Evil Twin Attack* yang dapat mengecoh pengguna untuk terhubung ke *access point* palsu. Penelitian ini bertujuan mengevaluasi kerentanan jaringan Wi-Fi Universitas Mataram terhadap serangan tersebut dengan model *multihop*, serta memberikan rekomendasi teknis untuk peningkatan keamanan. Metode yang digunakan adalah *penetration testing* etis menggunakan NodeMCU ESP8266 ber-*firmware Deauther*, dengan pengujian di 13 lokasi kampus. Variabel yang diamati meliputi jumlah perangkat terhubung, interaksi dengan halaman *phishing*, keberhasilan *deauthentication*, dan kredensial yang diperoleh. Hasil temuan kami menunjukkan lima dari 13 lokasi (38,46%) rentan, di mana pengguna berhasil diarahkan ke SSID palsu dan memasukkan kredensial, meskipun sebagian besar *deauthentication* gagal. Temuan ini menegaskan bahwa keberhasilan serangan tidak hanya ditentukan oleh *deauthentication*, tetapi juga dipengaruhi variasi *firmware* dan konfigurasi AP. Hasil temuan ini dapat menjadi dasar bagi pengelola jaringan untuk perlunya audit keamanan jaringan, pembaruan dan standarisasi *firmware*, penguatan autentikasi dengan enkripsi menyeluruh, serta peningkatan kewaspadaan pengguna terhadap *phishing*.

Kata kunci: *evil twin*; keamanan jaringan; wi-fi kampus; *multihop*; nodemcu esp8266

Abstract
The increasing use of Wi-Fi in higher education also brings security risks, such as Evil Twin Attacks that trick users into connecting to fake access points. This study aims to assess the vulnerability of Universitas Mataram's Wi-Fi network to such attacks using a multihop model and to propose technical improvements. An ethical penetration testing method was applied using a NodeMCU ESP8266 with Deauther firmware, tested across 13 campus locations. Observed variables included the number of connected devices, user interaction with phishing pages, deauthentication success, and captured credentials. The results reveal that five out of 13 locations (38.46%) were vulnerable, where users were redirected to fake SSIDs and entered credentials, even though most deauthentication attempts failed. These findings highlight that attack success depends not only on deauthentication but also on firmware variation and AP configuration. The study implies the need for network security audits, firmware standardization, stronger authentication with full encryption, and enhanced user awareness to reduce phishing risks.

Keywords**:** *evil twin; network security; campus wi-fi; multihop; nodemcu esp8266*

PENDAHULUAN

Perkembangan teknologi informasi mendorong peningkatan penggunaan Wi-Fi di perguruan tinggi karena akses yang mudah (Shaikh et al., 2025). Namun, kemudahan ini diiringi risiko keamanan (Ariyadi et al., 2024). Ditandai dengan meningkatnya serangan nirkabel seperti *Evil Twin* menurut laporan *Verizon* dan *Kaspersky* (Shi et al., 2025). Serangan

Edumatic: Jurnal Pendidikan Informatika is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

tersebut mampu mengecoh pengguna agar terhubung ke *access point* palsu, sehingga data sensitif dapat dicuri. Studi terbaru menegaskan bahwa deteksi *Evil Twin* dapat dilakukan melalui pendekatan data *mining* berbasis sinyal spektrum (Banakh et al., 2024). Fakta di lapangan menunjukkan kasus serupa pernah terjadi di STT Wastukancana, di mana jaringan kampus terbukti rentan terhadap pencurian kredensial (Sigit et al., 2024).

Keamanan jaringan bertujuan melindungi dan mengantisipasi ancaman yang mengganggu aktivitas jaringan (Zhang et al., 2021), termasuk serangan seperti *man in the middle*, *deauthentication*, rogue Wi-Fi, dan *Evil Twin* (Kaur & Dhiman, 2024). *Evil Twin Attack* merupakan teknik umum untuk memasuki jaringan dan memperoleh informasi korban (Dereli & Yildiz, 2024; Louca et al., 2023; Kara, 2024; Palamà et al., 2023), penyerang bahkan dapat mengeksploitasi protokol roaming 802.11v untuk meningkatkan keberhasilan serangan (Louca et al., 2023). Kondisi ini memudahkan pengambilalihan lalu lintas data korban, termasuk kredensial sensitif (Tian et al., 2021). Penerapan keamanan jaringan merupakan sebagai bagian dari sistem yang menjadi peningkatan untuk menjaga keamanan data dan integritas data (Jufri & Heryanto, 2021). Oleh karena itu, strategi proteksi seperti *Wireless Intrusion Detection*, enkripsi WPA3, serta segmentasi jaringan berbasis IP maupun MAC Address semakin diperlukan (Laksana & Mulyani, 2024).

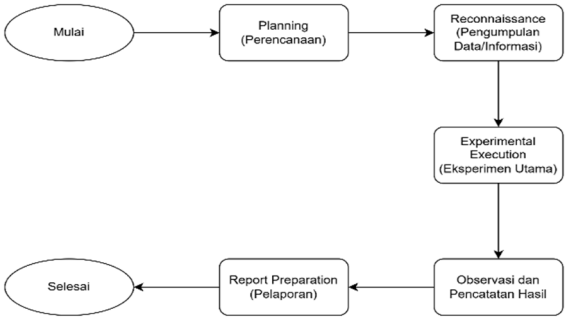
Permasalahan utama pada jaringan Wi-Fi kampus terletak pada lemahnya pertahanan *access point*, di mana meskipun dikelola secara terpusat, konfigurasi keamanan tidak selalu konsisten sehingga menimbulkan perbedaan kerentanan meski menggunakan pera. ngkat keras yang sama. Selain itu, metode autentikasi yang masih mengirimkan data *login* dalam format yang dapat ditangkap membuka peluang serangan berbasis rekayasa sosial maupun *packet* sniffing. Kondisi ini memungkinkan pencurian kredensial pengguna, seperti yang dapat terjadi melalui simulasi *Evil Twin* dengan NodeMCU ESP8266 yang menampilkan halaman login palsu untuk menjebak korban, sebagaimana ditunjukkan pada kasus di STT Wastukancana (Sigit et al., 2024). Sebagai salah satu cara untuk memahami permasalahan tersebut, kami memberikan solusi dengan melakukan simulasi serangan *Evil Twin* secara etis dengan menggunakan perangkat NodeMCU ESP8266, yaitu mikrokontroler yang berbasis Wi-Fi dan telah diprogram dengan *firmware* seperti *Deauther* (Alhamed, 2023).

Di Indonesia, kasus-kasus *Evil Twin* di lingkungan pendidikan masih jarang dilaporkan secara publik, namun hasil studi lokal menunjukkan adanya potensi kerentanan yang cukup tinggi. Penelitian sebelumnya yang dilakukan oleh Fikri et al. (2023) hanya meneliti kerentanan jaringan terhadap serangan *deauthentication* dengan NodeMCU ESP8266 tanpa menguji tahapan lanjutan *Evil Twin*, Aman (2023) berfokus pada simulasi *Man in the Middle* dan *Evil Twin* menggunakan Lapara Wi-Fi Master tetapi tidak membandingkan kerentanan antara lokasi dengan perangkat yang sama. Sementara itu Umasugi et al. (2022) menganalisis serangan *packet sniffing* dengan Ettercap dan Wireshark, namun tidak menguji variasi konfigurasi keamanan AP di lokasi berbeda. Oleh karna itu perlunya pengujian *Evil Twin* berbasis model *multihop* dengan NodeMCU ESP8266 secara langsung di lingkungan kampus guna mendapatkan hasil analisis mengenai jumlah perangkat yang terhubung ke AP palsu, interaksi dengan halaman phising, serta perbedaan konfigurasi keamanan antar lokasi. Kajian empiris semacam ini dapat memberikan gambaran yang lebih luas tentang kerentanan jaringan Wi-Fi di perguruan tinggi (da Silva et al., 2023; Andarini et al., 2023;).

Tujuan penelitian kami ini adalah untuk mengevaluasi kerentanan jaringan Wi-Fi Universitas Mataram terhadap *Evil Twin Attack* berbasis model *multihop*. Hasil yang diperoleh diharapkan menjadi dasar evaluasi teknis bagi pengelola dalam menyusun standar konfigurasi keamanan yang seragam, meningkatkan sistem autentikasi, serta memberikan wawasan kepada sivitas akademika agar lebih waspada terhadap ancaman serangan siber di lingkungan kampus.

METODE

Penelitian ini menggunakan pendekatan *penetration testing* etis untuk menguji kerentanan Wi-Fi di lingkungan kampus Universitas Mataram terhadap *Evil Twin* model multihop (Lina & Fernandes, 2022), dengan perangkat NodeMCU ESP8266 ber-*firmware Deauther* untuk mensimulasikan dua serangan. Pengujian dilakukan dengan izin dan koordinasi pengelola jaringan agar tidak mengganggu operasional, yang diawali dengan studi literatur dari buku, jurnal dan skripsi terkait keamanan jaringan dan *Evil Twin.* Pengujian dilakukan di beberapa gedung Kampus 1 Universitas Mataram, seperti LPPM, UPT Pusat Bahasa, UPT Perpustakaan, LPMPP, Fakultas Teknik, MIPA, Hukum, Ekonomi dan Bisnis, Pertanian, serta FKIP. Lokasi dipilih karena tingginya trafik saat perkuliahan, keberagaman tipe AP dengan model dan *firmware* berbeda, serta variasi kekuatan sinyal dan kepadatan pengguna. Penelitian menggunakan NodeMCU ESP8266 ber-*firmware Deauther* dan laptop (Windows 11, 8 GB RAM, *Ryzen* 3, SSD 236 GB). Adapun tahapan – tahapan yang akan dilakukan dalam penelitian ini yang sudah dipaparkan pada *flowchart* alur pelaksanaan penelitian yang ditampilkan pada gambar 1.



Gambar 1. *Flowchart* penelitian

Tahapan metode ini berdasarkan alur dari gambar 1, dimulai dengan perencanaan melalui observasi awal dan koordinasi dengan teknisi untuk menentukan lokasi uji yang aman. Dilanjutkan pengumpulan data awal berupa SSID, jenis AP, dan protokol keamanan sebagai dasar skenario pengujian. Tahap eksperimen menyalakan NodeMCU ESP8266 ber-*firmware Deauther* untuk membuat AP palsu, dan pada model multihop digunakan lebih dari satu perangkat untuk memperluas jangkauan serangan. Dilakukan pencatatan terhadap jumlah perangkat yang terhubung, interaksi pengguna pada halaman palsu, serta respon koneksi. Data yang diperoleh kemudian dianalisis untuk menilai efektivitas serangan berdasarkan jumlah perangkat yang menjadi target dan kredensial yang berhasil dikumpulkan.

Metode yang digunakan untuk pengujian dalam penelitian ini adalah metode *Evil Twin Attack Multihop*. Alur pengujian dimulai dari konfigurasi NodeMCU ESP8266 dengan *firmware Deauther* untuk memancarkan SSID palsu, mengirim paket *deauthentication* guna memutus koneksi korban, setelah koneksi terputus, korban diarahkan ke halaman *login* tiruan yang merekam kredensial. Dengan *multihop*, koneksi korban diteruskan ke jaringan asli agar pengguna tidak curiga. Data yang terekam kemudian dianalisis untuk mengevaluasi kerentanan pada *access point*.

HASIL DAN PEMBAHASAN

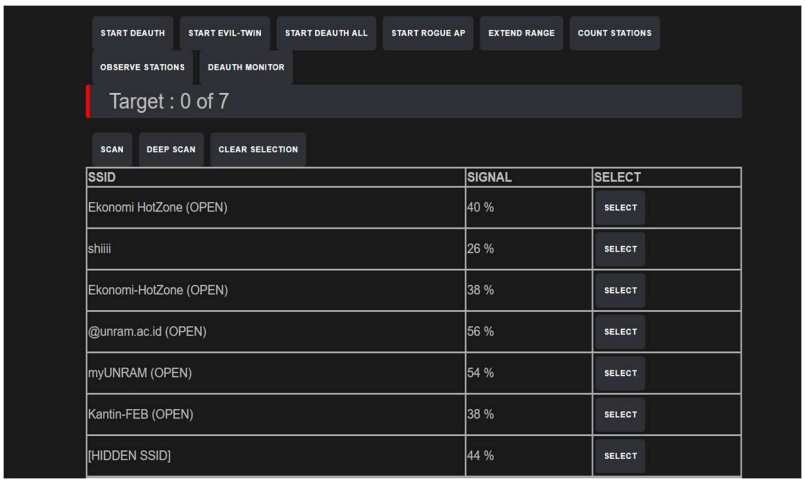
Hasil

Pada tahap *planning* diawali dengan observasi awal serta koordinasi dengan teknisi jaringan untuk menentukan lokasi pengujian yang aman agar tidak mengganggu operasional jaringan. Dari hasil observasi ditetapkan 13 lokasi pengujian yang tersebar di kampus 1 Universitas Mataram. Kemudian pada tahap *reconnaissance* bertujuan untuk mengumpulkan

data awal berupa SSID, jenis AP, serta protokol keamanan sebagai dasar skenario pengujian. Pada gambar 3 merupakan tahap awal untuk memulai pengujian *Evil Twin*.

Gambar 2. Koneksi laptop ke nodemcu esp8266

Gambar 2 menunjukkan proses menghubungkan laptop ke alat *Evil Twin Attack* untuk mengakses antarmuka *Deauther*, melalui Alamat IP bawaan perangkat. Proses ini merupakan tahap awal yang wajib berhasil agar serangan dapat dijalankan, karena dari tahap ini penyerang dapat mengontrol fungsi pemindaian SSID, pemancaran SSID palsu, hingga eksekusi serangan *deauthentication* dan *Evil Twin*.

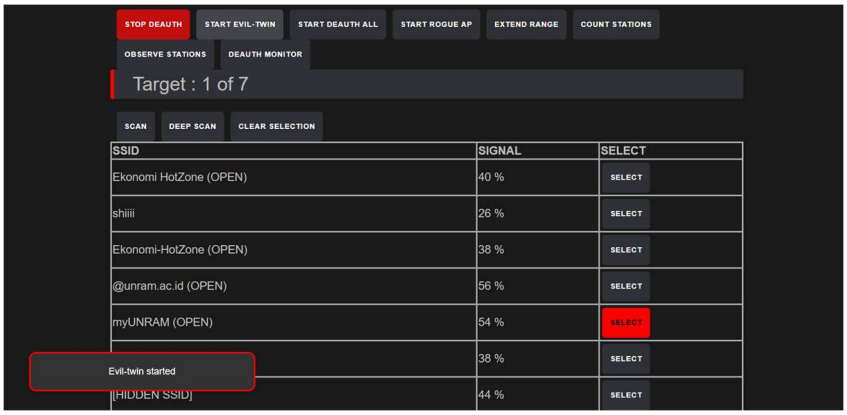


Gambar 3. *User interface evil twin attack*

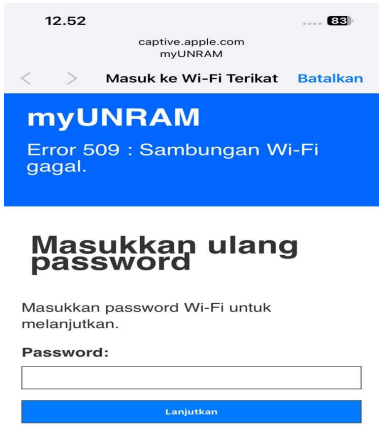
Pada gambar 3 adalah tampilan *user interface Evil Twin Attack*, halaman tersebut diakses dengan cara meng*input* IP *addres default software* yaitu "192.168.4.1" pada *browser*. Antarmuka ini menjadi pusat kendali seluruh proses serangan. Ketersediaan fitur seperti *Start Deauth* dan *Start Evil Twin* memungkinkan penguji memilih strategi yang sesuai. Tahap ini memiliki keberhasilan penuh di semua lokasi karena antarmuka berbasis web NodeMCU relatif stabil. Sebelum serangan dilakukan, terlebih dahulu dijalankan proses pemindaian SSID menggunakan fitur *scanning* untuk mengidentifikasi target dengan sinyal terkuat. Informasi tersebut menjadi dasar pemilihan AP yang akan diserang.

Selanjutnya pada gambar 4 memperlihatkan serangan dengan menekan *Start Deauth* dan *Start Evil Twin* setelah *scanning* SSID target; *Deauther* memutus koneksi korban dari AP asli, sedangkan NodeMCU ESP8266 menyiarkan SSID palsu seperti "@myUNRAM". Tahap

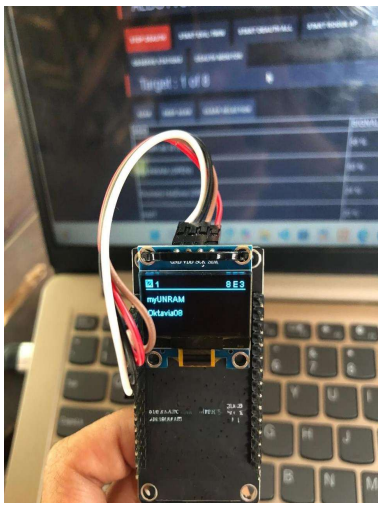
krusial ini menjalankan dua serangan sekaligus, dan pada lima lokasi Evil Twin berhasil meski deauth gagal karena korban mengenali SSID.



Gambar 4. Melakukan penyerangan



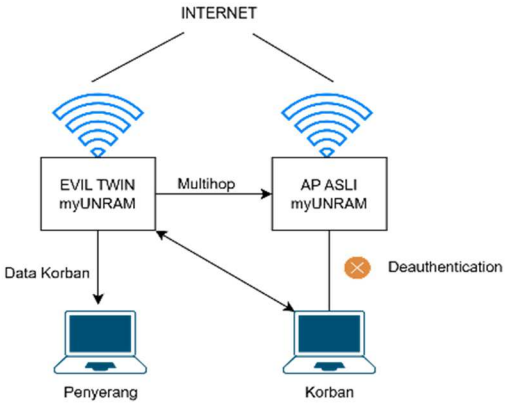
Gambar 5. Respon hasil wi-fi target



Gambar 6. Hasil *password*

Sementara itu, gambar 5 menunjukkan pengguna diarahkan ke halaman *login* palsu yang meniru SSID kampus "myUNRAM", Halaman ini menampilkan pesan "*Error* 509: Sambungan Wi-Fi gagal" untuk memancing korban memasukkan ulang kata sandi, Kredensial yang di masukkan kemudian secara otomatis disimpan atau dikirim ke penyerang. Tahap ini terbukti efektif pada beberaa lokasi pengujian yang rentan.

Gambar 6 memperlihatkan tahap akhir proses pengujian, di mana setelah korban terhubung ke access point palsu dan memasukkan kata sandi pada halaman login tiruan, informasi tersebut berhasil direkam melalui interface *Evil Twin*. Pada uji coba terhadap jaringan "myUNRAM", kata sandi "Oktavia08" berhasil diperoleh. Temuan ini menunjukkan bahwa serangan dapat berjalan efektif terhadap pengguna yang kurang waspada dan tidak memastikan keaslian jaringan sebelum melakukan *login*.



Gambar 7. Topologi serangan

Alur serangan *Evil Twin* berbasis *Multihop* Model yang disajikan pada gambar 7, di mana AP palsu meniru SSID asli, memutus koneksi korban lewat *deauthentication*, lalu mengarahkan ke halaman *login* tiruan untuk merekam kredensial. Dengan *multihop*, koneksi korban diteruskan ke AP asli sehingga internet tetap berjalan tanpa disadari, dan topologi ini menjadi dasar pengujian yang datanya ada pada tabel 1.

Hasil pada tabel 1 menunjukkan beberapa AP rentan terhadap *Evil Twin*. Semua menggunakan model *Ruijie* RG-AP720-L, namun variasi *firmware* memengaruhi hasil; Fakultas MIPA dengan versi AP_RGO S 11.1(9)B1 P19 aman dari kedua serangan. Peneliti memperoleh *password* melalui halaman *login* palsu namun gagal melakukan *deauthentication*. Lima dari 13 lokasi (38,46%) rentan, yaitu Gedung LPPM, Fakultas Hukum, Ekonomi dan Bisnis, Pertanian, serta Teknologi dan Pangan.

Hal tersebut menunjukkan bahwa walaupun pengguna telah diarahkan dan terhubung ke *access point* palsu, sistem keamanan *access point* tersebut tetap mampu menolak pemutusan koneksi secara paksa karna perangkat tersebut memiliki fitur yang dapat mendeteksi aktivitas jaringan yang mencurigakan sehingga dapat memberi tanda jika adanya serangan pada jaringan Wi-Fi termasuk serangan *deauthentication* dan *Evil Twin*. Sebaliknya delapan titik lokasi lainnya, seperti Fakultas Teknik, Fakultas MIPA, UPT. Perpustakaan, dan UPT. Pusat Bahasa, menunjukkan bahwa *access point* tidak rentan terhadap serangan tersebut, baik pada pemalsuan SSID maupun pemutusan koneksi atau dapat dikatakan jumlah lokasi yang sepenuhnya aman sebanyak 61,54%. Hal tersebut menunjukkan bahwa konfigurasi keamanan *access point* di lokasi-lokasi tersebut telah diperkuat melalui *firmware* terbaru.

Pada hasil pengujian yang telah dilakukan oleh peneliti bahwa jumlah rata-rata perangkat yang terhubung ke SSID palsu di lokasi rentan sebanyak 4 sampai 6 perangkat per lokasi. Jumlah total kredensial yang berhasil dikumpulkan sebanyak sebelas *password* unik dari total

angka rentang dua puluh sampai tiga puluh perangkat yang terkoneksi di seluruh lokasi rentan. Rata-rata waktu respon pengguna terhadap halaman login palsu rentang 10 sampai 15 detik sejak koneksi terputus atau diarahkan ke SSID palsu.

Tabel 1. Hasil pencatatan status *vulnerability*

Lokasi Perangkat	**Nama SSID Wi-Fi**	**Jenis *Access Point***	**Versi *Firmware***	**Hasil Pengujian**	
				Deauthentication	*Evil Twin*
Gedung LPPM	@myUNRAM	Ruijie RG-AP720-L	AP_RGO S 11.9(4)B1	Gagal	Berhasil
UPT. Pusat Bahasa	@myUNRAM	Ruijie RG-AP720-L	AP_RGO S 11.9(4)B1	Gagal	Gagal
UPT. Perpustakaan	@myUNRAM	Ruijie RG-AP720-L	AP_RGO S 11.9(4)B1	Gagal	Gagal
Gedung LPMPP	@myUNRAM	Ruijie RG-AP720-L	AP_RGO S 11.9(4)B1	Gagal	Gagal
Fakultas Teknik	@myUNRAM	Ruijie RG-AP720-L	AP_RGO S 11.9(4)B1	Gagal	Gagal
Fakultas MIPA	@myUNRAM	Ruijie RG-AP720-L	AP_RGO S 11.1(9)B1 P19	Gagal	Gagal
Fakultas Hukum	@myUNRAM	Ruijie RG-AP720-L	AP_RGO S 11.9(4)B1	Gagal	Berhasil
Fakultas Ekonomi dan Bisnis	@myUNRAM	Ruijie RG-AP720-L	AP_RGO S 11.9(4)B1	Gagal	Berhasil
Fakultas Pertanian	@myUNRAM	Ruijie RG-AP720-L	AP_RGO S 11.9(4)B1	Gagal	Berhasil
FKIP	@myUNRAM	Ruijie RG-AP720-L	AP_RGO S 11.9(4)B1	Gagal	Gagal
Fakultas Ilmu Komunikasi	@myUNRAM	Ruijie RG-AP720-L	AP_RGO S 11.9(4)B1	Gagal	Gagal
Fakultas Teknologi Dan Pangan	@myUNRAM	Ruijie RG-AP720-L	AP_RGO S 11.9(4)B1	Gagal	Berhasil
Fakultas Peternakan	@myUNRAM	Ruijie RG-AP720-L	AP_RGO S 11.9(4)B1	Gagal	Gagal

Pembahasan

Hasil penelitian menunjukkan bahwa beberapa titik jaringan Wi-Fi di Universitas Mataram masih rentan terhadap serangan Evil Twin, yang teridentifikasi melalui pengujian menggunakan NodeMCU ESP8266 dan perangkat lunak NETHERCAP. Gambar 2 memperlihatkan koneksi awal perangkat uji. Gambar 3 memperlihatkan antarmuka pengguna Evil Twin Attack yang menyediakan fitur Deauth dan Evil Twin, menandakan bahwa penyerang dapat memilih strategi sesuai kondisi jaringan. Gambar 4 menampilkan hasil pemindaian SSID target, yang berfungsi menentukan AP dengan sinyal terkuat agar korban lebih mudah diarahkan ke jaringan palsu.

Hasil pada gambar 5 menampilkan halaman login tiruan yang digunakan untuk menjebak korban agar memasukkan kredensial. Sementara itu, pada gambar 6 membuktikan keberhasilan pencatatan password melalui metode phishing. Selanjutnya, gambar 7 menggambarkan topologi multihop, di mana AP palsu tidak hanya menyalin SSID asli tetapi juga meneruskan koneksi ke jaringan sebenarnya sehingga korban tidak menyadari adanya serangan. Pendekatan multihop terbukti meningkatkan efektivitas serangan karena koneksi korban tetap diteruskan ke jaringan asli, sehingga pengguna tidak curiga meski terhubung ke AP palsu.

Tabel 1 menyajikan rekapitulasi hasil pengujian di 13 lokasi kampus. Data menunjukkan lima lokasi rentan (38,46%) dan delapan lokasi relatif aman (61,54%). Perbedaan hasil ini meski menggunakan perangkat AP yang sama (Ruijie RG-AP720-L) disebabkan oleh variasi firmware serta konfigurasi keamanan di tiap lokasi. Hal ini menegaskan bahwa faktor *firmware* dan pengaturan autentikasi menjadi kunci utama kerentanan.

Secara keseluruhan, temuan ini membuktikan bahwa meskipun sebagian besar *deauthentication* gagal karena fitur keamanan modern mampu menolaknya, serangan *Evil Twin* tetap berhasil melalui mekanisme *phishing* halaman *login*. Fakta tersebut memperlihatkan bahwa perlindungan jaringan tidak cukup hanya dengan menolak *deauthentication*, melainkan juga harus mencegah peniruan SSID dan pemalsuan halaman *login*. Oleh karena itu, pendekatan *multihop* yang digunakan dalam penelitian ini terbukti efektif dalam mengecoh pengguna, sekaligus mengungkap kelemahan mendasar dalam sistem keamanan Wi-Fi kampus.

Pada delapan lokasi, serangan *deauthentication* maupun halaman *login* palsu tidak berhasil. Menurut teknisi PUSTIK, meskipun seluruh *access point* (AP) Universitas Mataram dikelola melalui *Ruijie Cloud*, perbedaan tingkat kerentanan tetap terjadi karena faktor konfigurasi, perbedaan *firmware*, dan sinkronisasi kebijakan (Zhang et al., 2021). Dari sisi autentikasi, *login* myUNRAM memang menggunakan *token* terenkripsi, tetapi *username* dan password masih dikirim dalam format *plain text*, sehingga mudah direkam oleh alat seperti NETHERCAP. Temuan ini memperkuat hasil Umasugi et al. (2022) bahwa enkripsi menyeluruh sangat diperlukan untuk mencegah serangan berbasis *packet sniffing* dan rekayasa sosial.

Hasil temuan yang dilakukan oleh Fikri et al. (2023) hanya berfokus pada serangan *deauthentication*, penelitian kami memperluas ruang lingkup dengan menguji *Evil Twin* berbasis *multihop* sehingga mampu mengungkap kerentanan meskipun *deauthentication* gagal. Sementara itu, berbeda dengan Aman (2023) yang menyoroti *Man in the Middle* dan *Evil Twin* tanpa menganalisis konfigurasi AP, penelitian kami justru menekankan pengaruh variasi *firmware* dan sinkronisasi kebijakan keamanan antar lokasi. Lalu hasil temuan kami ini menyempurnakan temuan Umasugi et al. (2022) dengan menambahkan bukti empiris bahwa kredensial tetap dapat dicuri melalui phishing halaman login meskipun sebagian data telah dienkripsi.

Keterbatasan penelitian ini terletak pada lingkup uji yang hanya mencakup kampus Universitas Mataram dan penggunaan NodeMCU ESP8266 yang belum merepresentasikan seluruh teknik *Evil Twin* canggih. Meski demikian, hasilnya menegaskan perlunya audit keamanan berkala, edukasi pengguna terkait *phishing*, serta pengetatan kebijakan konfigurasi AP di lingkungan kampus.

SIMPULAN

Hasil penelitian ini menunjukkan bahwa sebagian jaringan Wi-Fi di Universitas Mataram, khususnya SSID "@myUNRAM", masih memiliki kerentanan terhadap serangan *Evil Twin*. Dari 13 lokasi yang diuji, lima lokasi (38,46%) terbukti rentan dengan pengguna berhasil diarahkan ke *access point* palsu dan memasukkan kredensial pada halaman *login*

tiruan, meskipun proses *deauthentication* tidak selalu berhasil karena adanya fitur deteksi aktivitas mencurigakan pada *access point*. Sementara itu, delapan lokasi lainnya (61,54%) relatif lebih aman berkat penggunaan *firmware* terbaru dan konfigurasi keamanan yang lebih kuat. Perbedaan hasil ini menegaskan bahwa faktor *firmware* dan pengaturan autentikasi berperan penting dalam tingkat kerentanan jaringan. Berdasarkan temuan tersebut, diperlukan langkah strategis berupa audit konfigurasi jaringan secara menyeluruh, pembaruan dan penyelarasan *firmware*, peningkatan keamanan autentikasi melalui enkripsi *end-to-end* dan penerapan HTTPS secara penuh, serta edukasi dan pelatihan bagi pengguna agar lebih waspada terhadap ancaman phishing.

REFERENSI

Abedi, A., Lu, H., Chen, A., Liu, C., & Abari, O. (2022). Wi-Fi physical layer stays awake and responds when it should not. *Proceedings of the ACM Workshop on Hot Topics in Wireless*, 35–42.

Alhamed, A. (2023). Ethical penetration testing for wireless networks: Identifying and mitigating Evil Twin vulnerabilities. *International Journal of Cybersecurity and Digital Forensics, 12*(3), 145–154.

Aman, A. (2023). Pengujian keamanan jaringan nirkabel melalui simulasi serangan Man in The Middle dan Evil Twin di sekolah XYZ. *Digital Transformation Technology (Digitech), 3*(2), 824–831. https://doi.org/10.47709/digitech.v3i2.3378

Andarini, R., Prasetyo, M., & Wulandari, E. (2023). Peningkatan keamanan sistem informasi berbasis jaringan nirkabel di perguruan tinggi. *Jurnal Teknologi Informasi dan Komputer, 8*(1), 45–53.

Ariyadi, T., Irwansyah, & Huda, M. S. (2024). Analisis keamanan jaringan Wi-Fi mahasiswa UBD dari serangan packet sniffing. *Jurnal Ilmiah Informatika, 12*(1), 53–58. https://doi.org/10.33884/jif.v12i01.8739

Banakh, M., Korol, O., & Sokolov, A. (2024). Data mining approach for Evil Twin attack identification in Wi-Fi networks. *Data, 9*(10), 119. https://doi.org/10.3390/data9100119

da Silva, P., Costa, H., & Ribeiro, L. (2023). Experimental evaluation of Evil Twin attacks in higher education Wi-Fi environments. *International Journal of Information Security Science, 12*(2), 55–66.

Dereli, T., & Yildiz, M. (2024). Twin ghosts: Evil Twin attacks in wireless networks and defense mechanisms. *Bilecik Şeyh Edebali University Journal of Science, 11*(1), 85–96.

Fikri, L. M. Z., Zafrullah, A., & Zubaidi, A. (2023). Analisis keamanan jaringan Wi-Fi dengan metode deauthentication attack pada access point di lingkungan Universitas Mataram. *Jurnal Teknologi dan Sistem Informasi, 11*(2), 75–84.

Jufri, M., & Heryanto. (2021). Peningkatan keamanan jaringan wireless dengan menerapkan security policy pada firewall. *JOISIE (Journal of Information Systems and Informatics Engineering), 5*(2), 98–108. https://doi.org/10.35145/joisie.v5i2.175

Kara, İ. (2024). Twin Ghosts: Evil Twin Attacks in Wireless Networks and Defense Mechanisms. *Bitlis Eren University Journal of Science and Technology*, *14*(2), 58-74. https://doi.org/10.17678/beuscitech.1450756

Kaur, G., & Dhiman, R. (2024). Detecting and preventing rogue access points in wireless networks: A survey. *International Journal of Network Security, 26*(4), 412–422.

Laksana, T. G., & Mulyani, S. (2024). Pengetahuan dasar identifikasi dini deteksi serangan kejahatan siber untuk mencegah pembobolan data perusahaan. *Jurnal Ilmiah Multidisiplin, 3*(1), 109–122. https://doi.org/10.56127/jukim.v3i01.1143

Lina, I. M., & Fernandes, G. R. (2022). Analisis pola social engineering menggunakan teknik Wi-Fi deauther dan Evil Twin. *JRKT (Jurnal Rekayasa Komputasi Terapan), 2*(4), 253–260. https://doi.org/10.30998/jrkt.v2i04.8185

Louca, A., Constantinou, D., & Georgiou, A. (2023). Exploiting 802.11v mechanisms for enhanced Evil Twin attacks. *Proceedings of the IEEE International Conference on Communications (ICC)*, 1–6.

Louca, C., Peratikou, A., & Stavrou, S. (2023). A novel Evil Twin MiTM attack through 802.11 v protocol exploitation. *Computers & Security*, *130*, 103261. https://doi.org/10.1016/j.cose.2023.103261

Palamà, I., Amici, A., Bellicini, G., Gringoli, F., Pedretti, F., & Bianchi, G. (2023). Attacks and vulnerabilities of Wi-Fi Enterprise networks: User security awareness assessment through credential stealing attack experiments. *Computer Communications*, *212*, 129-140. https://doi.org/10.1016/j.comcom.2023.09.031

Riyanti, E., & Sutejo, A. (2024). Strategi pengamanan jaringan nirkabel terhadap ancaman serangan MITM dan Evil Twin. *Jurnal Keamanan Siber, 4*(1), 33–42.

Shaikh, F., Shaikh, H., & Shah, M. (2025). Review of Evil Twin attacks in the age of Wi-Fi 6 and WPA3: An evaluation of threats, techniques, and technological responses. *IRE Journals, 8*(11), 45–52.

Shi, L., Hernandez, J., & Zhang, W. (2025). A survey on secure Wi-Fi sensing technology: Attacks and defenses. *Sensors, 25*(6), 1913. https://doi.org/10.3390/s25061913

Sigit, M., Singasatia, D., & Kurniawan, I. (2024). Pengujian serangan Evil Twin ESP8266 pada wireless networking dengan metode penetration testing (Studi kasus: STT Wastukancana). *Jurnal Ilmiah Sain dan Teknologi, 2*(11), 193–214.

Tian, Y., Wang, S., & Zhang, L. (2021). Convolutional neural network based Evil Twin attack detection in Wi-Fi networks. *MATEC Web of Conferences, 336*, 08006. https://doi.org/10.1051/matecconf/202133608006