Journal of Information Technology and Computer Science (INTECOMS)
Volume 9 Nomor 2, Tahun 2026
e-ISSN : 2614-1574
p-ISSN : 2621-3249

IDENTIFIKASI CELAH KEAMANAN JARINGAN NIRKABEL TERHADAP SERANGAN EVIL TWIN MENGGUNAKAN METODE NETWORK SCANNING

IDENTIFICATION OF WIRELESS NETWORK SECURITY VULNERABILITIES AGAINST EVIL TWIN ATTACKS USING NETWORK SCANNING METHODS

Fahmi Romisa[1], Ruqoyyah Nasution[2], Sukemi[3]
Universitas Mulawarman, Samarinda, Kalimantan Timur[1,2,3]
romy@fkip.unmul.ac.id[1]

ABSTRACT

Wireless network security remains a critical issue due to the rise of Man-in-the-Middle (MitM) threats, specifically via Evil Twin attacks. This attack operates by duplicating a legitimate Service Set Identifier (SSID) to deceive users into connecting to a rogue access point. This study aims to identify the vulnerabilities of wireless network infrastructures toward Evil Twin penetration by implementing network scanning methods. The research methodology encompasses data packet scanning stages (ping sweeps and port scanning) to detect anomalies in MAC addresses and Signal Strength. The results demonstrate that the proactive use of network scanning tools effectively detects the presence of unauthorized access points attempting data interception. These findings contribute to the development of more robust wireless security protocols and provide technical recommendations for network administrators in mitigating the risks of sensitive information theft.
Keywords*: Network Security, Evil Twin, Network Scanning, Access Point, Vulnerability.*

ABSTRAK

Keamanan jaringan nirkabel tetap menjadi isu krusial seiring meningkatnya ancaman serangan Man-in-the-Middle (MitM), khususnya melalui metode Evil Twin. Serangan ini bekerja dengan menduplikasi Service Set Identifier (SSID) yang sah untuk mengelabui pengguna agar terhubung ke titik akses palsu. Penelitian ini bertujuan untuk mengidentifikasi kerentanan infrastruktur jaringan nirkabel terhadap penetrasi Evil Twin dengan mengimplementasikan metode network scanning. Metodologi penelitian mencakup tahap pemindaian paket data (ping sweep dan port scanning) untuk mendeteksi anomali pada alamat MAC dan kekuatan sinyal (Signal Strength). Hasil penelitian menunjukkan bahwa penggunaan alat pemindaian jaringan secara proaktif mampu mendeteksi keberadaan titik akses asing yang mencoba melakukan intersepsi data. Temuan ini memberikan kontribusi pada pengembangan protokol keamanan nirkabel yang lebih tangguh dan memberikan rekomendasi teknis bagi administrator jaringan dalam memitigasi risiko pencurian informasi sensitif.
Kata Kunci: Keamanan Jaringan, Evil Twin, Network Scanning, Titik Akses, Kerentanan

PENDAHULUAN

Pertumbuhan infrastruktur jaringan nirkabel yang masif di era transformasi digital saat ini membawa konsekuensi pada meningkatnya risiko keamanan siber. Salah satu ancaman paling persisten dan sulit dideteksi secara konvensional adalah serangan Evil Twin. Teknik ini memanfaatkan manipulasi psikologis dan teknis dengan menduplikasi identitas titik akses (Access Point) legal untuk menjerat pengguna.

Identifikasi masalah dalam penelitian ini berfokus pada:

- Ketidakmampuan pengguna awam dalam membedakan antara SSID asli dengan Access Point bayangan yang dikendalikan penyerang.
- Kurangnya mekanisme deteksi dini pada sisi klien maupun administrator jaringan terhadap anomali transmisi data yang bersifat interceptor.
- Kebutuhan akan metode verifikasi yang lebih proaktif, seperti pemindaian jaringan (network scanning), untuk memetakan keberadaan entitas asing dalam ekosistem nirkabel.

Penerapan Keamanam jaringan nirkabel merupakan sebuah sistem yang digunakan untuk meindentifikasi dan melakukan pencegahan pencurian data dan informasi pada jaringan komputer. (Santoso dkk., 2022). sementara itu menurut (Irfan dkk., 2024) Keamanan jaringan merupakan prosedur perlindungan sistem yang berfokus pada pemantauan

akses pengguna yang sah di dalam jaringan, Strategi pengendaliannya sering kali dianalisis melalui kerangka manajemen risiko. Salah satu instrumen penting dalam ekosistem ini adalah Wireless Intrusion Detection System (WIDS), yang mencakup sekumpulan alat dan metodologi untuk mengidentifikasi serta melaporkan berbagai aktivitas dalam jaringan komputer nirkabel.

Istilah keamanan Internet merujuk pada upaya proteksi menyeluruh terhadap transaksi dan pertukaran informasi di ruang siber. Fokus utamanya adalah menjamin keamanan akses web, integritas input data pengguna, serta kerahasiaan transmisi data melalui Internet Protocol. Keamanan tersebut ditegakkan melalui tiga komponen infrastruktur vital: DNS, TCP/IP, dan Interdomain Routing (Sampetoding dkk., 2020). Transformasi teknologi yang masif memberikan dampak besar terhadap dimensi sosial, ekonomi, dan kultural, namun secara bersamaan memperluas celah kerentanan terhadap infiltrasi virus, tindakan pirasi, serta berbagai ancaman siber lainnya (Azzahra dkk., 2024).

Keamanan jaringan nirkabel kini menjadi perhatian utama yang memerlukan penanganan serius. Hal ini dikarenakan media transmisinya menggunakan gelombang radio yang dipancarkan secara terbuka, sehingga sinyal tersebut bergerak bebas di ruang udara dan rentan diintersepsi oleh pihak mana pun tanpa batasan waktu (Samsumar & Gunawan, 2017).

Dalam hal penanganan dalam institusi menurut (Pratama, 2023). Penggunaan Virtual Private Network (VPN) telah menjadi standar bagi banyak organisasi untuk mengenkripsi pertukaran informasi internal antar lokasi. Selain itu, VPN berperan krusial dalam memitigasi risiko keamanan ketika karyawan melakukan akses data perusahaan melalui jaringan publik saat bekerja remote.

Integrasi teknologi nirkabel berbasis standar IEEE 802.11 telah menjadi pilar utama dalam mendukung konektivitas global yang fleksibel dan efisien. Meskipun aspek performa transmisi data terus mengalami akselerasi, penguatan pada sektor keamanan seringkali tertinggal, terutama pada Data Link Layer. Karakteristik transmisi nirkabel yang bersifat broadcast menyebabkan sinyal radio sangat rentan terhadap intersepsi oleh entitas luar, sehingga memperluas spektrum ancaman bagi integritas data di ruang publik maupun privat.

Salah satu bentuk ancaman yang paling krusial dan sulit diidentifikasi secara kasat mata adalah infiltrasi melalui metode Evil Twin. Berbeda dengan teknik serangan siber konvensional yang mencoba menjebol enkripsi, strategi Evil Twin lebih memfokuskan pada manipulasi mekanisme otentikasi antara user dan Access Point (AP). Penyerang mengonfigurasi titik akses replika yang memiliki atribut identik dengan jaringan orisinal, seperti manipulasi alamat MAC (BSSID), kesamaan identitas SSID, serta penggunaan kanal frekuensi yang berhimpitan.

Kerentanan ini semakin diperburuk oleh algoritma pemilihan jaringan otomatis pada perangkat seluler modern, yang secara algoritmis lebih memprioritaskan kekuatan sinyal (signal strength) dibandingkan verifikasi sertifikat keamanan AP. Dampaknya, pengguna dapat terjebak dalam skenario Man-in-the-Middle (MitM), di mana seluruh lalu lintas data dapat disadap, dimodifikasi, atau digunakan untuk mencuri kredensial melalui teknik phishing yang canggih.

Dalam upaya mitigasi risiko tersebut, pemetaan celah keamanan melalui metode Network Scanning menjadi prosedur audit yang sangat mendesak. Dengan memanfaatkan teknik pemindaian proaktif maupun observasi pasif, pengelola jaringan mampu melakukan survei lingkungan frekuensi radio untuk mendeteksi keberadaan Rogue Access Point. Penulisan ini memfokuskan pada ekstraksi parameter teknis, seperti fluktuasi Received Signal Strength Indication (RSSI), inkonsistensi nomor urut paket data, serta anomali pada

struktur beacon frames, yang berfungsi sebagai indikator utama untuk memvalidasi keaslian sebuah infrastruktur nirkabel.

Keamanan informasi berfokus pada upaya perlindungan data serta sistem pendukungnya dari berbagai ancaman, seperti akses ilegal, modifikasi tanpa izin, hingga perusakan oleh pihak yang tidak berwenang. Tujuannya adalah menjamin tiga aspek utama: kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Keamanan ini ditopang oleh empat pilar utama, yaitu organisasi, sumber daya manusia, proses, serta teknologi, yang saling berinteraksi melalui elemen manajemen, budaya, hingga dukungan teknis (Nurul dkk., 2022).

Kendati protokol WPA3 mulai diadopsi secara luas, faktanya banyak sistem yang masih beroperasi pada standar WPA2 atau bahkan jaringan tanpa proteksi yang menjadi sasaran empuk serangan kloning identitas. Studi ini diarahkan untuk membedah variabel kerentanan pada jaringan nirkabel serta mengevaluasi sejauh mana kapabilitas Network Scanning dalam mengidentifikasi kehadiran serangan Evil Twin secara akurat. Output dari analisis ini diharapkan mampu memberikan kontribusi teknis dalam perancangan sistem proteksi nirkabel yang lebih tangguh dan adaptif terhadap ancaman kontemporer.

METODE

Penelitian ini menerapkan metodologi kualitatif deskriptif yang disusun secara sistematis. Proses identifikasi kerentanan pada jaringan nirkabel dilakukan melalui integrasi tahapan pengumpulan data dan penetration testing guna memperoleh analisis keamanan yang komprehensif. (Sigit dkk., 2024)

Pada tahap awal, metode scanning dilakukan secara pasif maupun aktif untuk mengidentifikasi seluruh Access Point (AP) yang berada dalam jangkauan. Parameter yang dipindai meliputi:

- SSID (Service Set Identifier): Nama jaringan yang terlihat oleh pengguna.
- BSSID (Basic Service Set Identifier): Alamat MAC fisik dari router/AP.
- Channel: Frekuensi yang digunakan (misalnya 2.4 GHz atau 5 GHz).
- Signal Strength (RSSI): Kekuatan sinyal untuk menentukan posisi relatif AP.

Metode scanning di sini bertujuan untuk mencari duplikasi atau "kembaran" dari jaringan resmi. Peneliti mencari indikator serangan Evil Twin melalui:

- Duplicate SSID: Adanya dua jaringan dengan nama yang sama persis namun memiliki BSSID yang berbeda.
- MAC Spoofing Detection: Scanning untuk melihat apakah ada AP yang mencoba meniru alamat MAC resmi tetapi memiliki karakteristik sinyal atau enkripsi yang berbeda.
- Evil Twin Identification: Menggunakan alat seperti Airodump-ng atau Kismet untuk memantau apakah ada lonjakan paket Deauthentication yang memaksa pengguna terputus dari AP asli dan pindah ke AP palsu.

Penetration testing atau pentesting merupakan prosedur simulasi serangan yang bertujuan untuk mengidentifikasi kerentanan, ancaman, serta risiko pada sistem komputer, jaringan, maupun aplikasi. Dalam konteks jaringan nirkabel, metode ini berperan penting dalam memperkuat infrastruktur, seperti penguatan konfigurasi firewall pada router. Adapun kerentanan (vulnerability) didefinisikan sebagai celah akibat kelemahan desain, konfigurasi, atau perangkat lunak yang berpotensi dieksploitasi oleh pihak tidak bertanggung jawab. Fokus utama pentesting adalah mendeteksi titik lemah tersebut secara dini, sehingga pemilik sistem dapat melakukan langkah mitigasi sebelum terjadi eksploitasi oleh penyerang (Okario, 2023).

HASIL DAN PEMBAHASAN

Tahap awal penelitian difokuskan pada pemetaan parameter dasar jaringan nirkabel dalam kondisi operasional normal. Melalui teknik Passive Monitoring, dilakukan ekstraksi data terhadap Access Point (AP) yang menjadi subjek uji coba. Observasi ini krusial untuk menetapkan standar perbandingan terhadap aktivitas anomali di kemudian hari.

Tabel 1. Spesifikasi Teknis

Parameter	Nilai / Deskripsi
BSSID (MAC Address)	00:14:22:01:12:30
Channel	6 (2.412 GHz)
Encryption	WPA2-PSK (AES)
Rata-rata RSSI	-45 dBm hingga -50 dBm

Serangan disimulasikan dengan membuat AP tiruan menggunakan perangkat alat ESP8266MOD,

Gambar 1. Wifi Evil Twin

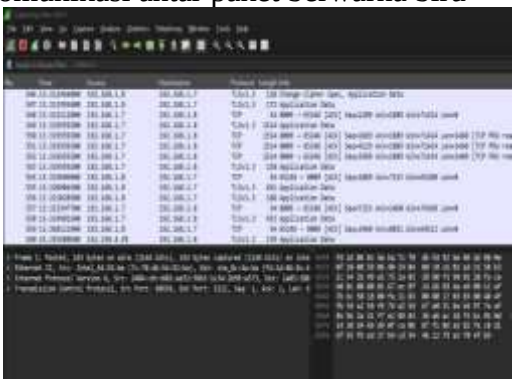
Penyerang mengkloning SSID dan BSSID yang sama dengan target.

Gambar 2. Memilih wifi target

Hasil pemindaian menunjukkan bahwa saat serangan aktif, terdapat wifi memiliki nama ibrahim dan tidak memiliki internet yang berguna untuk menjebak korban untuk masuk sedangkan wifi utama tidak bisa di akses karna sudah dilakukan proses deauth wifi.

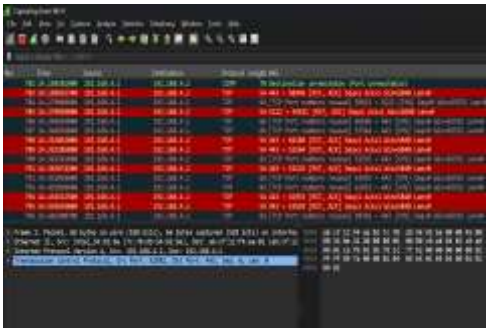
Simulasi gangguan keamanan diimplementasikan dengan memproyeksikan sebuah titik akses bayangan yang mereplikasi identitas AP resmi secara presisi. Data pemindaian menunjukkan terjadinya duplikasi identitas digital di lingkungan udara yang sama, menciptakan ambiguitas bagi perangkat klien.

Eksploitasi diawali dengan transmisi paket Deauthentication secara masif. Berdasarkan inspeksi trafik menggunakan penganalisis paket, ditemukan lonjakan transmisi yang sesuai pada wifi utama yaitu koneksi antar jaringan dapat berkomunikasi secara normal yang di tandai dengan setiap komunikasi antar paket berwarna biru



Gambar 3. Hasil Scan Wifi Utama

Sedangkan hasil scan pada wifi evil twin terdapat anomali koneksi antar paket jaringan yang ditandai dengan komunikasi berwarna merah.



Gambar 4. Hasil Scan Wifi Evil Twin

.

Data hasil pemindaian aktif menyingkap adanya diskrepansi pada kekuatan sinyal radio. Walaupun kedua node memiliki SSID yang identik, sistem pemindai mendeteksi perbedaan intensitas yang signifikan:

- Wifi utama: Mempertahankan stabilitas sinyal pada kisaran -48 dBm.
- Wifi Evil Twin: Menghasilkan pancaran lebih dominan pada -30 dBm untuk menarik minat perangkat klien secara otomatis.

Analisis mendalam terhadap struktur Beacon Frames mengungkap adanya ketidakkonsistenan pada nomor urut paket (Sequence Number). Dalam kondisi normal, urutan ini bersifat inkremental dan linear. Namun, kehadiran Evil Twin menyebabkan terjadinya lompatan angka yang tidak sinkron dalam log pemindaian. Hal ini mengindikasikan adanya dua proses hardware berbeda yang mencoba menyiarkan identitas yang sama.

Analisis: Temuan ini mengonfirmasi bahwa algoritma pemilihan jaringan pada standar 802.11 memiliki kelemahan fundamental, di mana prioritas konektivitas lebih ditentukan oleh faktor fisik (kekuatan sinyal) daripada autentikasi kredensial penyedia layanan.

SIMPULAN

Berdasarkan rangkaian eksperimen dan prosedur penetration testing yang telah dilaksanakan, penelitian ini berhasil memetakan profil kerentanan pada ekosistem jaringan nirkabel standar 802.11 terhadap ancaman serangan Evil Twin. Secara fundamental, temuan ini mengonfirmasi bahwa kelemahan utama keamanan Wi-Fi bukan hanya terletak pada protokol enkripsi (seperti WPA2/WPA3), melainkan pada mekanisme pemilihan jaringan otomatis (Auto-Connect) yang bersifat agnostik terhadap otentikasi identitas fisik perangkat keras.

Pertama, hasil analisis menunjukkan bahwa metode Network Scanning secara proaktif merupakan instrumen deteksi dini yang sangat efektif. Melalui parameter Received Signal Strength Indication (RSSI), peneliti menemukan anomali signifikan di mana Access Point (AP) palsu yang menggunakan perangkat ESP8266MOD sengaja memancarkan sinyal yang lebih dominan (berkisar -30 dBm) dibandingkan AP orisinal (-48 dBm). Hal ini mengeksploitasi algoritma perangkat klien modern yang cenderung memprioritaskan "kedekatan fisik" sinyal untuk menjamin stabilitas koneksi, sehingga tanpa sadar menjerat pengguna ke dalam skenario Man-in-the-Middle (MitM).

Kedua, melalui inspeksi mendalam terhadap struktur paket data menggunakan penganalisis paket, penelitian ini berhasil mengidentifikasi diskrepansi teknis pada Beacon Frames. Inkonsistensi pada Sequence Number (nomor urut paket) yang tidak lagi bersifat linear menjadi indikator kuat adanya dualitas transmisi pada identitas BSSID yang sama. Lebih lanjut, keberhasilan simulasi serangan yang diawali dengan injeksi paket Deauthentication secara masif membuktikan betapa rapuhnya ketersediaan (availability) layanan jaringan nirkabel saat ini.

DAFTAR PUSTAKA

Azzahra, N. S., Tambunan, A. M., Aulia, N. N., Binarsih, A., & Saepudin, T. H. (t.t.). *TINJAUAN LITERATUR TENTANG ANCAMAN CYBERCRIME DAN IMPLEMENTASI KEAMANAN SIBER DI INDUSTRI PERBANKAN*.

Irfan, A., Nusri, A. Z., Rachmat, Z., & Wulandari, S. (2024). Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System (WIDS). *Jurnal Ilmiah Sistem Informasi dan Teknik Informatika (JISTI)*, *7*(1), 110–119. https://doi.org/10.57093/jisti.v7i1.195

Nurul, S., Shynta Anggrainy, & Siska Aprelyani. (2022). FAKTOR-FAKTOR YANG

MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM). *Jurnal Ekonomi Manajemen Sistem Informasi*, *3*(5), 564–573. https://doi.org/10.31933/jemsi.v3i5.992

Okario, A. (2023). *Analisis Celah Keamanan Jaringan WPA dan WPA2 Dengan Menggunakan Metode Penetration Testing*. *1*.

Pratama, R. (t.t.). *Literature Review: Network Security Menggunakan Virtual Private Network L2TP/IPSEC, Port Knocking, Port Forwarding, Honeypot Dan Pfsense*.

Sampetoding, E. A. M., Natalin, M., Manapa, E. S., Yoga, V., & Ardhana, P. (2020). *Studi Literatur: Cara Kerja Keamanan Internet dan Kerentanan dengan TCP/IP dan DNS*.

Samsumar, L. D., & Gunawan, K. (2017). ANALISIS DAN EVALUASI TINGKAT KEAMANAN JARINGAN KOMPUTER NIRKABEL (WIRELESS LAN); STUDI KASUS DI KAMPUS STMIK MATARAM. *Jurnal Ilmiah Teknologi Infomasi Terapan*, *4*(1). https://doi.org/10.33197/jitter.vol4.iss1.2017.152

Santoso, N. A., Ainurohman, M., & Kurniawan, R. D. (t.t.). *PENERAPAN METODE PENETRATION TESTING PADA KEAMANAN JARINGAN NIRKABEL*.

Sigit, M., Singasatia, D., Kom, S., Kom, M., Kurniawan, I., & Kom, M. (2024). *PENGUJIAN SERANGAN EVIL TWIN ESP8266 PADA WIRELESS NETWORKING DENGAN METODE PENETRATION TESTING (STUDI KASUS: SEKOLAH TINGGI TEKNOLOGI WASTUKANCANA)*.