JURNAL ILMIAH SISTEM INFORMASI (JUSI)
VOL 5, No. 1, Januari 2026, pp. 257 - 274
p-ISSN : 2803-1507 (media cetak) | e-ISSN : 2803-1531 (media online)
Link Publikasi: https://ejurnal.provisi.ac.id/index.php/JUISI/issue/view/169

Security Evaluation of WPA2 vs WPA3 Wireless Network Against Deauthentication and Brute Force Attacks using Aircrack-ng

Harry Pribadi Fitrian[1], Eri Eriyana[2], Hendrick Maulana Ibrahim*[3], Riordan Pramana Rizqullah[4], Silvia Putri Meliansyah[5]
[1,2,3,4,5] Program Studi S1 Informatika, Universitas Teknologi Digital, Bandung, Indonesia
Jl. Cibogo Indah No. 3, kode pos 40000, Kota Bandung, Provinsi Jawa Barat, Indonesia
e-mail: harrypribadi@digitechuniversity.ac.id[1], sayaeriiii@gmail.com[2],
hendrickmaulanaibrahim@gmail.com*[3], riordan2704@gmail.com[4], silviaputrim30@gmail.com[5]

ARTICLE INFO

Article History:

Received: 28-11-2025
Revised: 15-12-2025
Accepted: 09-01-2026
Published: 21-01-2026

ABSTRACT

Wireless network security has become a critical issue amid the proliferation of Wireless Local-Area Networks (WLAN) *across various sectors. Although the theoretical superiority of* WPA3-SAE *has been documented in the literature, a significant gap remains in comparative empirical validation using standardized penetration testing methodology—particularly in measuring resilience against deauthentication and dictionary attacks, which represent the most prevalent attack vectors. This research fills this gap through controlled ethical penetration testing with multi-vendor configuration and quantifiable security metrics. Findings demonstrate fundamental architectural disparity:* WPA2-PSK *with optional Protected Management Frames* (PMF) *exhibits systemic vulnerability to both attack vectors, while* WPA3-SAE *with mandatory* PMF *and Simultaneous Authentication of Equals* (SAE) *demonstrates full resilience. This research contributes to the body of knowledge through: (1) empirical validation of* PMF *effectiveness in preventing management frame manipulation in real-world scenarios, (2) a quantitative comparative framework for measuring protocol vulnerabilities, and (3) evidence-based recommendations for wireless security governance. The findings reinforce the theoretical proposition that the security-by-design approach is fundamentally superior to security-by-retrofit, with strategic implications for information security policy in modern organizations.*

Keywords: *Wireless Security*, *WPA2-PSK*, *WPA3-SAE*, *Penetration Testing*, *Deauthentication Attack.*

Abstrak

Keamanan jaringan nirkabel menjadi isu kritis seiring proliferasi *Wireless Local-Area Network* (WLAN) di berbagai sektor. Meskipun superioritas teoretis WPA3-SAE telah didokumentasikan dalam literatur, *gap* signifikan tetap ada dalam validasi empiris komparatif menggunakan *standardized penetration testing methodology* khususnya dalam mengukur *resilience* terhadap *deauthentication* dan *dictionary attacks* yang merupakan *attack vectors* paling *prevalent*. Penelitian ini mengisi *gap* tersebut melalui *ethical penetration*

DOI: https://doi.org/10.51903/gy968e07

p-ISSN : 2803-1507 e-ISSN : 2803-1531

testing terkontrol dengan *multi-vendor configuration* dan *quantifiable security metrics*. Temuan mendemonstrasikan disparitas arsitektural fundamental: WPA2-PSK dengan *optional Protected Management Frames* (PMF) menunjukkan kerentanan sistemik terhadap kedua *attack vectors*, sementara WPA3-SAE dengan *mandatory* PMF dan *Simultaneous Authentication of Equals* (SAE) menunjukkan resistensi penuh. Penelitian ini berkontribusi pada *body of knowledge* melalui: (1) validasi empiris efektivitas PMF dalam mencegah management frame manipulation di *real-world scenarios*, (2) *framework* komparatif kuantitatif untuk mengukur *protocol vulnerabilities*, dan (3) *evidence-based recommendations* untuk *wireless security governance*. Temuan memperkuat proposisi teoretis bahwa s*ecurity-by-design approach* secara fundamental superior dibanding *security-by-retrofit*, dengan implikasi strategis untuk *information security policy* di organisasi modern.

Kata Kunci: *Wireless Security*, *WPA2-PSK, WPA3-SAE*, *Penetration Testing*, *Deauthentication Attack.*

1. PENDAHULUAN

Dengan berkembangnya teknologi jaringan komputer yang begitu pesat [1], [2], [3], terciptanya *Wireless Local-Area Network* (WLAN) tak hanya digunakan oleh pengguna rumahan namun digunakan juga oleh institusi pendidikan dan korporat , yang memudahkan pengguna untuk terhubung ke internet tanpa menggunakan kabel fisik [4]. Meski dengan kemudahan itu, tak lepas dari ancaman keamanan jaringan [5]. Oleh karena itu, perlindungan terhadap jaringan WLAN menjadi sebuah keharusan untuk mencegah akses yang tidak diizinkan dan ancaman penyalahgunaan data pengguna [6]. Dengan adanya celah itulah*, Institute of Electrical and Electronics Engineers* (IEEE) menetapkan standar keamanan 802.11, dengan empat protokol untuk mengamankan jaringan WLAN, yaitu *Wired Equivalent Privacy* (WEP), *Wi-Fi Protected Access* (WPA), *Wi-Fi protected Access 2* (WPA2) dan paling baru adalah protokol *Wi-Fi Protected Access 3* (WPA3) [7]. Saat ini, penggunaan protokol WEP dan WPA sudah ditinggalkan, karena dua protokol tersebut memiliki celah keamanan yang mudah untuk dieksploitasi oleh peretas [8].

WEP menggunakan algoritma enkripsi RC4 dan bersifat statis, algoritma ini sangat lemah dalam implementasinya. Karena pada kasus ini, WEP memiliki panjang kunci sebanyak 24 bit, memungkinkan peretas menggunakan teknik *brute-force attack* dalam perhitungan menit untuk mendapatkan sebuah *password*. WPA menggunakan kunci yang dinamis, dengan panjang kunci sebanyak 128 bit. Algoritma pada WPA masih menggunakan algoritma RC4 dengan penambahan algoritma TKIP. Meski sudah ada penambahan algoritma enkripsi baru, WPA tetap dapat diretas. Metode penyerangannya adalah *Handshake-attack* dan *Denial of Service* (DoS) / *Deauthentication* jenis serangan ini menargetkan WLAN dengan cara memaksa memutus jaringan pengguna untuk mendapatkan handshake korban, setelah terputus dari jaringan, penyerang akan mendapatkan handshake korban untuk dianalisis dan selanjutnya digunakan untuk mendapatkan password korban, [9], [10], [11]. Oleh karena itu, penggunaan WPA2 dan WPA3 dinilai lebih aman dibandingkan protokol keamanan sebelumnya.

Meski standar keamanan sudah dikembangkan, standar ini tak luput dari celah keamanan yang dapat dieksploitasi oleh peretas [12]. Salah satu alat yang digunakan untuk meretas adalah sistem operasi *open source*, seperti Kali Linux dari distribusi sistem operasi gratis ini menjadi pilihan utama bagi *black-hat hacker* untuk meretas sebuah jaringan, dalam Kali Linux alat yang sering digunakan untuk meretas *adalah Aircrack-ng suite* [13], [14]. Meskipun WPA3 telah memiliki peningkatan sistem keamanan enkripsi yang signifikan melalui protokol *Simultaneous Authentication of Equals* (SAE) yang membuatnya jauh lebih sulit untuk diretas dibandingkan protokol keamanan sebelumnya, penelitian terbaru menunjukkan bahwa protokol ini masih rentan terhadap eksploitasi meskipun tingkat kerumitannya jauh lebih tinggi dibandingkan dengan serangan pada WPA [10]. WPA3 juga belum sepenuhnya kebal terhadap serangan seperti *downgrade* dan *side-channel*.

Hasil pengujian penetrasi membuktikan bahwa WPA3 memang jauh lebih sulit dieksploitasi dibandingkan WPA2, namun tetap memerlukan peningkatan untuk mencegah ancaman siber modern [15]. Selain itu, penelitian terbaru menunjukkan bahwa serangan Wi-Fi tidak hanya berfokus pada pencurian kata sandi, tetapi juga pada upaya pemutusan koneksi pengguna secara paksa (*Deauthentication Attack*) yang kemudian dapat dimanfaatkan untuk melakukan serangan lanjutan seperti *Evil Twin* dan pencurian kredensial melalui *fake captive portal*. Serangan ini menjadi ancaman yang sering ditemukan pada jaringan publik maupun institusi pendidikan karena dapat dilakukan tanpa harus mengetahui kata sandi jaringan, sehingga menimbulkan risiko kebocoran data pengguna secara luas [16], [17]. Oleh karena itu, penelitian ini bertujuan

p-ISSN : 2803-1507 e-ISSN : 2803-1531

menjawab pertanyaan : Seberapa efektif WPA2 dan WPA3 dalam mencegah serangan *Deauthentication* dan *brute-force.*

2. TINJAUAN PUSTAKA

2.1. *Evolusi Protokol Keamanan Wi-Fi*

Keamanan jaringan nirkabel telah mengalami evolusi signifikan sejak diperkenalkannya standar IEEE 802.11. Protokol keamanan Wi-Fi berkembang dari WEP (*Wired Equivalent Privacy*) yang memiliki kelemahan kriptografi fundamental [18], hingga WPA (*Wi-Fi Protected Access*) yang menggunakan TKIP, dan kemudian WPA2 yang mengadopsi enkripsi AES-CCMP [4], [15], [17], [19]. WPA2 menjadi standar keamanan yang paling banyak digunakan sejak 2004, menggunakan enkripsi AES (*Advanced Encryption Standard*) dengan mode CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) yang memberikan keamanan lebih kuat dibandingkan pendahulunya. Namun, seiring berkembangnya Teknik peretasan, WPA2 menunjukkan berbagai kerentanan yang mengancam keamanan jaringan nirkabel [4].

2.2. *Kerentanan WPA2 terhadap Serangan Modern*

2.2.1. *Serangan Deauthentication*

Serangan *deauthentication* merupakan ancaman yang telah ada sejak awal pengembangan Wi-Fi, Dimana penyerang bertujuan memutus koneksi klien dari jaringan dengan menyebabkan *denial of service*. Dalam serangan ini, Alamat MAC dari *access point* yang bertanggung jawab mengirim *frame deauthentication* di spoof, kemudian *frame deauthentication* palsu diinjeksikan untuk memaksa pengguna meninggalkan jaringan [19], [20]. Protected Management Frames (PMF) diperkenalkan melalui amandemen IEEE 802.11w dan diwajibkan pada WPA3, dengan tujuan meningkatkan perlindungan terhadap robust management frames melalui penyediaan *confidentiality, integrity, origin authenticity*, dan *replay protection* [4], [18], [19]. Meskipun demikian, penelitian terbaru menunjukkan bahwa PMF tidak cukup untuk mencegah serangan *deauthentication* sepenuhnya. [19] mengindentifikasi bahwa serangan deauthentication masih efektif sebelum pembentukan *4-way handshake*, dan menemukan kontradiksi dalam aturan standar IEEE 802.11 untuk memproses *frame deauthentication* dan *disassociation*.

2.2.2. *Serangan Dictionary dan Brute Force*

Protokol WPA2-PSK rentan terhadap serangan *dictionary offline* [4]. Cara kerja protokol ini menurunkan session key yang disebut *pairwise transitional key* (PTK) dari *random numbers* yang dipertukarkan dalam *4-way handshake*, yaitu *network name* (SSID), *Authenticator Nonce* (ANonce), *Supplicant Nonce* (SNonce), Alamat MAC pengguna, dan Alamat MAC *access point* [4], [15], [16], [17], [18], [19], [21].

2.3. *WPA3:Peningkatan Keamanan dan Protokol SAE*

WPA3 diperkenalkan oleh *Wi-Fi Alliance* pada tahun 2018 sebagai pengganti WPA2, dengan tujuan utama meningkatkan keamanan handshake WPA2-PSK. Protokol ini memiliki dua mode operasi: WPA3-Personal dan WPA3-Enterprise, dengan peningkatan signifikan pada mekanisme autentikasi dan manajemen kunci [4]. WPA3-Personal menggunakan *Simultaneous Authentication of Equals* (SAE), juga dikenal sebagai *Dragonfly handshake*, untuk autentikasi dan manajemen kunci. Pada WPA3-Personal, autentikasi dan manajemen kunci dilakukan melalui *Simultaneous Authentication of Equals (SAE)*, atau *Dragonfly handshake*, yang memanfaatkan *shared password* (PSK) antar pihak yang terlibat dalam proses *handshake*. Proses autentikasi SAE menghasilkan *paired master key* (PMK) yang akan digunakan sebagai input untuk *4-way handshake* guna membuat 192-bit PTK, yang lebih baik dibandingkan panjang kunci 128-bit pada WPA2 [4], [22].

SAE dirancang lebih kuat daripada PSK yang digunakan pada WPA2 dan memberikan proteksi terhadap serangan *dictionary* dan *brute force*. Mekanisme SAE menggunakan pertukaran kunci berbasis *Diffie-Hellman* untuk menurunkan kunci sesi, sehingga penyerang dapat meng-intersep data *handshake*, mereka tidak dapat menggunakan Kembali kunci sesi tersebut. Setiap sesi menghasilkan kunci baru, memberikan proteksi terhadap serangan *KRACK* dan serangan replay lainnya yang menjadi kerentanan pada WPA2 [4], [23].

2.4. *Tools Penetration Testing untuk Keamanan Wi-Fi*

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Dalam berbagai penelitian keamanan jaringan nirkabel, Aircrack-ng banyak digunakan sebagai tools pendukung security auditing untuk mengevaluasi kerentanan jaringan wireless melalui aktivitas penangkapan lalu lintas, injeksi paket, serta analisis dan pemulihan kata sandi. Suite ini mencakup beberapa tool penting : *airodump-ng* untuk menangkap dan monitoring lalu lintas WLAN, *aireplay-ng* untuk menghasilkan traffic dan mengirimkan paket deauthentication frame, serta aircrack-ng untuk melakukan *brute-force attack* dan *password recovery* dari *captured handshakes* [4], [24]. Penelitian oleh Cathcart dan Khan Mohd menganalisis lima *tool password cracking* di kali linux melalui serangan berbasis *dictionary.* Studi tersebut menyimpulkan bahwa *aircrack-ng* dan *wifite* memberikan analisis serangan yang lebih lengkap *dibandingkan hydra, fern wifi cracker,* dan *hashcat* dalam hal kecepatan, efisiensi, kompleksitas, desain, dan versatilitas [4], [25].

2.5. *Penelitian Terkait Penetration Testing WPA2 dan WPA3*

Wang et al. melakukan *penetration test* terhadap jaringan *Wi-Fi* yang menggunakan enkripsi WPA2, dengan mengusulkan metode serangan menggunakan *toolkit aircrack-ng* dari kali linux. Penelitian tersebut menunjukkan bahwa *password Wi-Fi* dapat diperoleh dengan cepat melalui laptop berkecepatan tinggi setelah mencoba beberapa *password* menggunakan *dictionary*, memberikan keuntungan dalam hal kesederhanaan, kecepatan, dan stabilitas [4], [26]. Kohlios dan Hayajneh melakukan studi teoritis komprehensif terhadap kemungkinan serangan pada standar keamanan Wi-Fi terbaru. Studi tersebut menyimpulkan bahwa WPA3 tidak terpengaruh oleh serangan deauthentication, *dictionary attack*, dan *KRACK*, namun serangan *Evil Twin* masih dimungkinkan. Temuan menarik dari penelitian ini Adalah bahwa setelah penetrasi jaringan local yang mendukung WPA3, jaringan masih kurang dalam mengatasi semua masalah yang ditemukan pada WPA2, terutama serangan *Man In The Middle* [4], [27].

2.6. *Research Gap*

Berdasarkan tinjauan literatur yang telah dilakukan, teridentifikasi beberapa kesenjangan penelitian yang mendasari urgensi studi ini:

2.6.1. *Keterbatasan Pengujian Praktis WPA3*

Sebagian besar penelitian tentang WPA3 bersifat analitis dan teoritis, dengan kurangnya pengujian penetrasi praktis terhadap protokol ini. Penelitian yang ada lebih banyak focus pada analisis keamanan WPA2, sementara pengujian empiris terhadap *robustness* WPA3 menggunakan *tools penetration testing* umum masih terbatas [4].

2.6.2. *Efektivitas PMF terhadap Serangan Deauthentication*

Meskipun PMF dirancang untuk melindungi terhadap serangan *deauthentication*, penelitian menunjukkan bahwa proteksi ini tidak sepenuhnya efektif, terutama pada fase sebelum *4-way handshake*. Diperlukan penelitian lebih lanjut untuk mengevaluasi efektivitas PMF dalam *scenario real world* dan mengidentifikasi kondisi spesifik Dimana PMF dapat di *bypass* [4], [28], [29].

2.6.3. *Perbandingan Komprehensif Kerentanan*

Belum ada penelitian yang secara komprehensif membandingkan kerentanan WPA2 dan WPA3 terhadap serangan *common* (*deauthentication* dan *dictionary attack*) dalam satu *framework* pengujian yang sama. Penelitian ini akan mengisi gap tersebut dengan melakukan *comparative analysis* menggunakan *tools* yang sama pada kedua protokol [4].

2.6.4. *Penggunaan Tools Serupa untuk WPA3*

Sebagian *tools* penetrasi yang ada, seperti *aircrack-ng*, dirancang untuk menyerang WPA2. Belum banyak penelitian yang menguji apakah *tools* tersebut masih efektif terhadap WPA3, terutama dalam konteks serangan *dictionary* dan *deauthentication*. Penelitian ini akan mengevaluasi efektivitas *aircrack-ng* terhadap WPA3 yang masih jarang digunakan secara global [4].

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental komparatif dengan metode *penetration testing* dalam lingkungan laboratorium tertutup yang telah mendapat izin resmi. Metode ini diterapkan untuk mengevaluasi ketahanan protokol WPA2-PSK dan WPA3-SAE terhadap serangan *deauthentication* dan *brute-force*. Perbandingan difokuskan pada respons protokol ketika menghadapi upaya pemutusan koneksi serta kemungkinan pemulihan kata sandi dari material autentikasi yang berhasil diperoleh.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

3.1. *Perangkat Pengujian*

3.1.1. *Sistem Perangkat Penyerangan (Attacking Device System)*

Perangkat penyerang menggunakan laptop dengan prosesor Intel Core i5-7300U dan memori RAM 8GB. Spesifikasi ini dipilih karena mencerminkan perangkat dengan kemampuan komputasi menengah yang masih mudah diakses secara luas, sehingga hasil penelitian dapat merepresentasikan ancaman realistis dari *adversary* dengan *resource* terbatas. Untuk mendukung proses pengujian, digunakan *adapter wifi* eksternal dengan chipset Atheros AR9271. Chipset ini memiliki dukungan *monitor mode* dan *packet injection* yang diperlukan dalam manipulasi *management frame* pada jaringan nirkabel.

3.1.2. *Platform Pengujian (Testing Platform)*

Sistem operasi yang digunakan adalah Kali Linux versi 2024.4, sebuah *platform* standar dalam *penetration testing* yang menyediakan *environment* terkontrol untuk *security assesment*. Pemilihan *platform* ini didasarkan pada compliance terhadap metodologi NIST SP 800-115 serta kemampuan reproduksibilitas yang memungkinkan validasi *indenpenden* terhadap temuan penelitian. Pengujian memanfaatkan Aircrack-ng suite versi 1.7 sebagai *framework* utama untuk evaluasi kerentanan protokol *wireless*. Pemilihan *tool* ini didasarkan pada tiga pertimbangan akademik : (1) validasi ekstensif dalam penelitian sejenis yang menunjukkan *reliability* dalam *wireless security assessment*, (2) kemampuan menghasilkan *output* terstruktur yang dapat dianalisis secara kuantitatif, dan (3) representasi *realistic attack scenarios* yang menggunakan *publicly-available tools*, mencerminkan *actual threat landscape* yang dihadapi organisasi. *Tool* suite ini mencakup komponen untuk *passive reconnaissance, active attack simulation*, dan *cryptographic analysis*, memungkinkan evaluasi komprehensif terhadap *attack surface* protokol yang di uji [4], [24], [25].

Wireshark digunakan sebagai *network protocol analyzer* untuk validasi *independen* terhadap *packet-level* behavior, memberikan visibilitas terhadap *protocol state transitions* dan *frame integrity verification mechanisms*. Analisis *dual-layer* ini (*attack simulation* dan *protocol analysis*) meningkatkan validity temuan melalui triangulasi metodologis. Pada tahap *dictionary attack*, digunakan *wordlist* berisi 300.00 *entri* yang merepresentasikan *common password patterns* sesuai OWASP *password testing guidelines*. Ukuran *wordlist* ini dipilih untuk *balance* antara *comprehensive coverage* terhadap *weak passwords* dan *feasibility computational time*, memungkinkan *quantifiable assessment* terhadap *brute-force resistance* dalam *time frame* yang *realistic* untuk *adversary* dengan *moderate resources*.

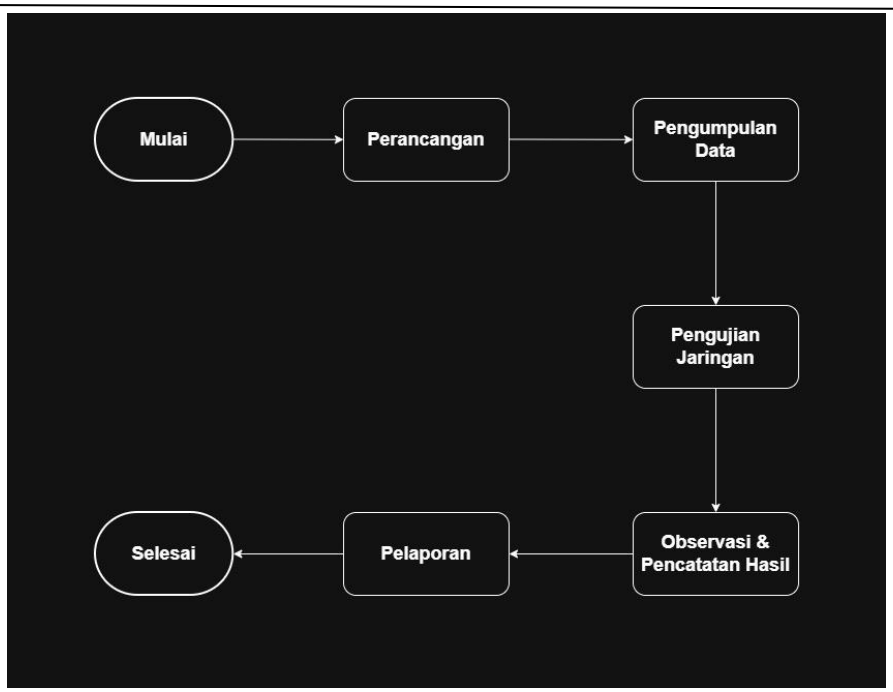
3.1.3. *Target Pengujian (Target Environment)*

Lingkungan pengujian terdiri dari dua *access point* yang dikonfigurasi dengan parameter jaringan identik, meliputi SSID dan *channel* yang sama. Penggunaan konfigurasi identik ini memungkinkan isolasi variabel protokol keamanan sebagai faktor tunggal yang mempengaruhi hasil pengujian. Perbedaan hanya terletak pada protokol keamanan WPA2-PSK untuk AP pertama dan WPA3-SAE untuk AP kedua. Kedua *access point* menggunakan kata sandi identik (bandung764) agar perbedaan hasil pengujian tidak dipengaruhi oleh variasi kekuatan kata sandi. Seluruh pengujian dilakukan pada jaringan yang terisolasi dari interferensi eksternal.

3.2. *Tahap Penelitian*

Adapun tahapan-tahapan yang akan dilakukan dalam penelitian ini, dipaparkan pada diagram *flowchart* dari penelitian ini yang ditampilkan pada Gambar 1.

p-ISSN : 2803-1507 e-ISSN : 2803-1531



Gambar 1. Flowchart penelitian

Tahapan penelitian dimulai dengan persiapan lingkungan pengujian dan pengumpulan informasi awal. Informasi yang dikumpulkan meliputi SSID, alamat MAC, *channel*, serta jenis protokol keamanan yang digunakan. Data ini menjadi dasar dalam penyusunan skenario serangan. Tahap berikutnya adalah pelaksanaan serangan *deauthentication* dan *brute-force* pada masing-masing protokol. Hasil pengujian kemudian dianalisis berdasarkan durasi serangan dan tingkat keberhasilannya.

3.3. *Skenario Metode Penyerangan*

Skenario pengujian dirancang untuk mengevaluasi ketahanan WPA2-PSK dan WPA3-SAE terhadap serangan *deauthentication* dan *brute-force* dalam kondisi yang terkontrol. Pengujian melibatkan satu *access point*, satu perangkat *client*, dan satu perangkat penyerang. Pada tahap awal (*reconnaissance*), dilakukan *monitoring* jaringan untuk mengidentifikasi parameter jaringan yang relevan. Tahap selanjutnya adalah serangan *deauthentication* dengan mengirimkan *management frame* palsu kepada *client* yang sedang terhubung. Pada protokol WPA2, serangan ini menyebabkan *client* terputus dan melakukan koneksi ulang. Pada protokol WPA3, serangan yang sama tetap diujikan, namun respons protokol menunjukkan adanya mekanisme proteksi terhadap *management frame* yang tidak sah. Ketika *client* melakukan koneksi ulang, dilakukan upaya penangkapan *handshake*. Material autentikasi yang berhasil diperoleh kemudian digunakan sebagai input untuk pengujian *brute-force* menggunakan *dictionary attack*. Proses ini bertujuan mengevaluasi kemungkinan pemulihan kata sandi serta kebutuhan waktu komputasi yang diperlukan.

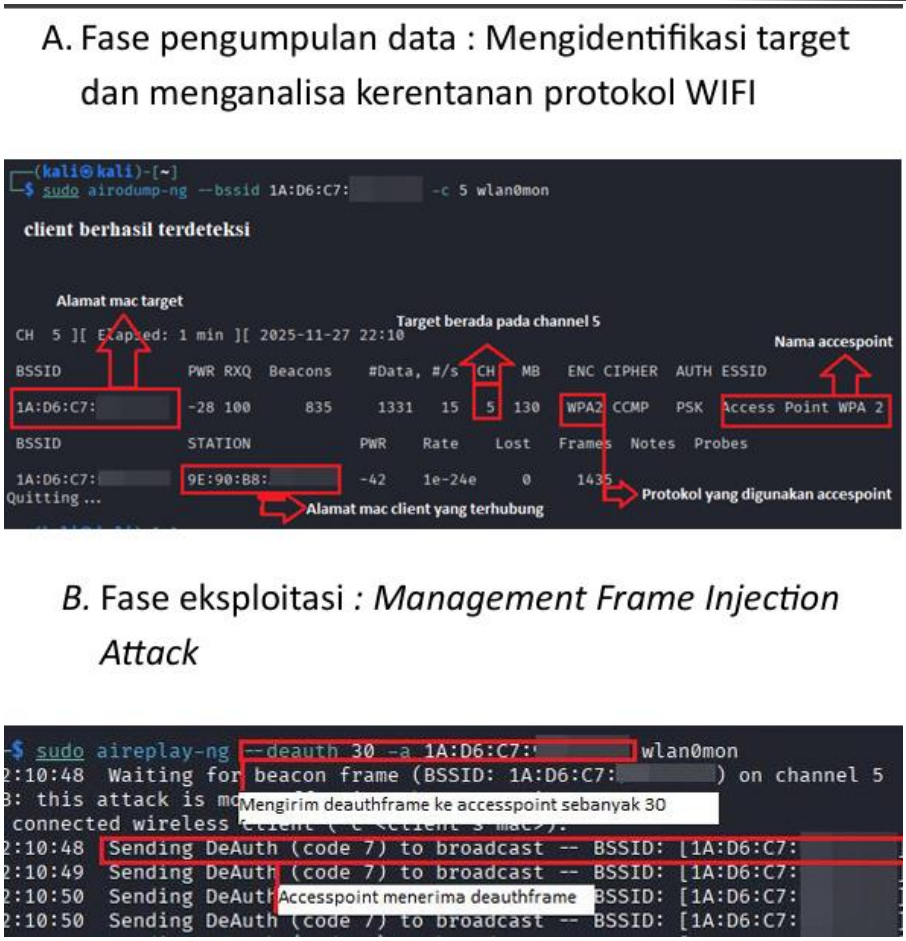
4. HASIL DAN PEMBAHASAN

Berdasarkan metode penelitian yang telah dipaparkan pada bagian metode penelitian, dilakukan eksperimen terhadap jaringan WPA2 PSK dan WPA3 SAE menggunakan *Aircrack-ng suite* dan *wireshark* sebagai alat analisis jaringan.

4.1. *Analisis Jaringan WPA2*

Pada tahap awal penelitian ini dilakukan proses *monitoring* terhadap jaringan WPA2-PSK untuk mengamati kondisi komunikasi antara *access point* dan *client* sebelum adanya serangan. Proses ini bertujuan untuk memperoleh gambaran awal mengenai stabilitas koneksi serta aktivitas jaringan yang berjalan secara normal. Data yang diperoleh pada tahap ini menjadi acuan pembanding untuk menganalisis perubahan perilaku jaringan setelah dilakukan pengujian keamanan. Hasil pengamatan awal terhadap kondisi jaringan WPA2-PSK tersebut ditunjukkan pada Gambar 2.

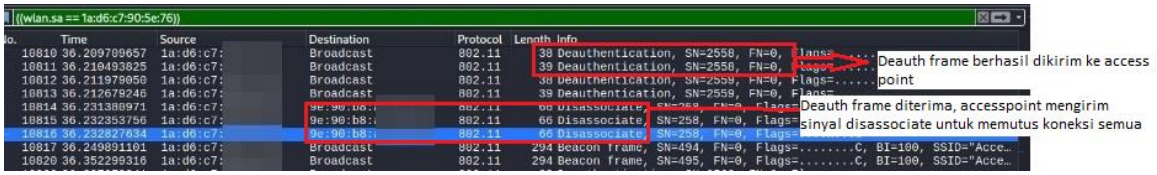
p-ISSN : 2803-1507 e-ISSN : 2803-1531



Gambar 2. Hasil Monitoring Jaringan WPA2-PSK menggunakan Airodump-ng

Gambar 2 menunjukan kondisi awal jaringan sebelum dilakukan penyerangan terhadap *access point.* Pada tahap ini, *access point* dan satu *client* berada dalam keadaan terhubung secara normal. Penetapan kondisi awal ini digunakan sebagai dasar analisis untuk memastikan bahwa perubahan perilaku jaringan tahap berikutnya merupakan dampak langsung dari serangan yang dilakukan, bukan akibat dari pemutusan jaringan yang bersifat insiden. Setelah *deauthframe* dikirimkan dan *acces point* menerima paket tersebut, koneksi *client* mengalami pemutusan tanpa adanya autentikasi ulang. Kondisi ini menunjukan bahwa serangan bekerja pada lapisan kontrol komunikasi, bukan hanya pada lapisan pelindung data. Dampak utama dari serangan ini adalah terganggunya koneksitivitas jaringan *wifi*, meskipun keamanan data tetap berjalan semestinya.

Setelah dilakukan pengiriman *deauthentication* dan *disassociation frame*, tahap selanjutnya adalah menganalisis paket jaringan untuk memastikan penyebab terputusnya koneksi klien. Analisis ini dilakukan menggunakan *packet analyzer* untuk mengamati respons yang diberikan oleh *access point* terhadap *management frame* yang diterima. Melalui proses ini dapat diketahui apakah pemutusan koneksi terjadi akibat pemrosesan frame manajemen atau disebabkan oleh faktor lain di luar mekanisme kontrol jaringan. Hasil analisis paket deauthentication dan disassociation frame pada jaringan WPA2-PSK tersebut ditunjukkan pada Gambar 3.



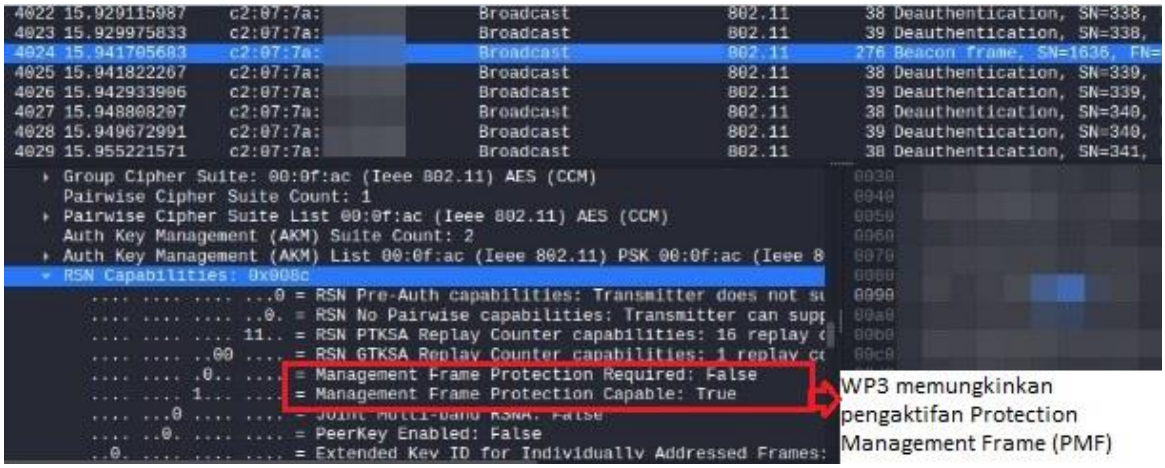
Gambar 3. Analisis Paket Deauthentication & Disassociation Frame pada Jaringan WPA2-PSK

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Untuk memastikan bahwa pemutusan koneksi terhadap *client* benar-benar disebabkan oleh pemrosesan *management frame*, Gambar 3 digunakan. Hasil dari analisis paket wireshark menujukan *access point* tetap merespon *deauth frame* yang diterima. Ini menunjukan bahwa *management frame* masih diproses tanpa mekanisme perlindungan yang memadai. Akibatnya, koneksi klien dapat terganggu meskipun tidak ada upaya untuk menembus enkripsi pada jaringan.

4.2. *Analisis Jaringan WPA3*

Pada tahap ini dilakukan proses *monitoring* terhadap jaringan WPA3-SAE untuk mengamati respons jaringan terhadap serangan *deauthentication* yang sama seperti pada pengujian WPA2. Pengujian ini bertujuan untuk membandingkan tingkat ketahanan jaringan WPA3 terhadap serangan pada *management frame* serta mengevaluasi efektivitas mekanisme keamanan yang diterapkan. Seluruh proses pengamatan dilakukan dalam kondisi jaringan yang stabil dan *client* terhubung secara normal. Hasil monitoring jaringan WPA3-SAE beserta responsnya terhadap serangan *deauthentication* ditunjukkan pada Gambar 4.



Gambar 4. Hasil Monitoring Jaringan WPA3-SAE dan kegagalan Serangan Deauthentication

Gambar 4 menunjukan pada jaringan WPA3 dengan fitur *Protected Management Frames* (PMF) aktif, Meskipun deauthentication frame telah dikirimkan, tidak terjadi pemutusan koneksi pada *client*. Perilaku ini menunjukkan bahwa mekanisme *Protected Management Frames* (PMF) pada WPA3 berfungsi dengan baik dalam mencegah serangan *deauthentication.*

Mekanisme proteksi ini bekerja pada tingkat protokol melalui beberapa lapisan keamanan: Pertama, PMF mengimplementasikan *Management Frame Protection* berdasarkan IEEE 802.11w yang mewajibkan enkripsi dan autentikasi kriptografis terhadap *management frame* kategori robust (termasuk *deauthentication* dan *disassociation frame*). Setiap *management frame* yang dikirimkan harus dilindungi menggunakan *Broadcast/Multicast Integrity Protocol* (BIP) untuk *frame broadcast* atau CCMP (*Counter Mode with CBC-MAC Protocol*) untuk *frame unicast*, yang menggunakan kunci turunan dari *Pairwise Master Key* (PMK) hasil SAE *handshake* [4], [19].

Kedua, setiap *management frame* yang terproteksi memiliki *Message Integrity Check* (MIC) yang dihitung menggunakan kunci sesi aktif. Ketika access point menerima *deauthentication frame*, protokol akan memverifikasi: (1) apakah *frame* memiliki MIC yang valid, (2) apakah MIC dihitung dengan kunci sesi yang benar, dan (3) apakah *sequence counter* sesuai untuk mencegah *replay attack*. Dalam serangan yang dilakukan, *deauthentication frame* palsu dikirim tanpa MIC yang valid atau menggunakan kunci yang tidak sesuai dengan sesi aktif, sehingga verifikasi kriptografis gagal pada tahap validasi integritas [19], [20].

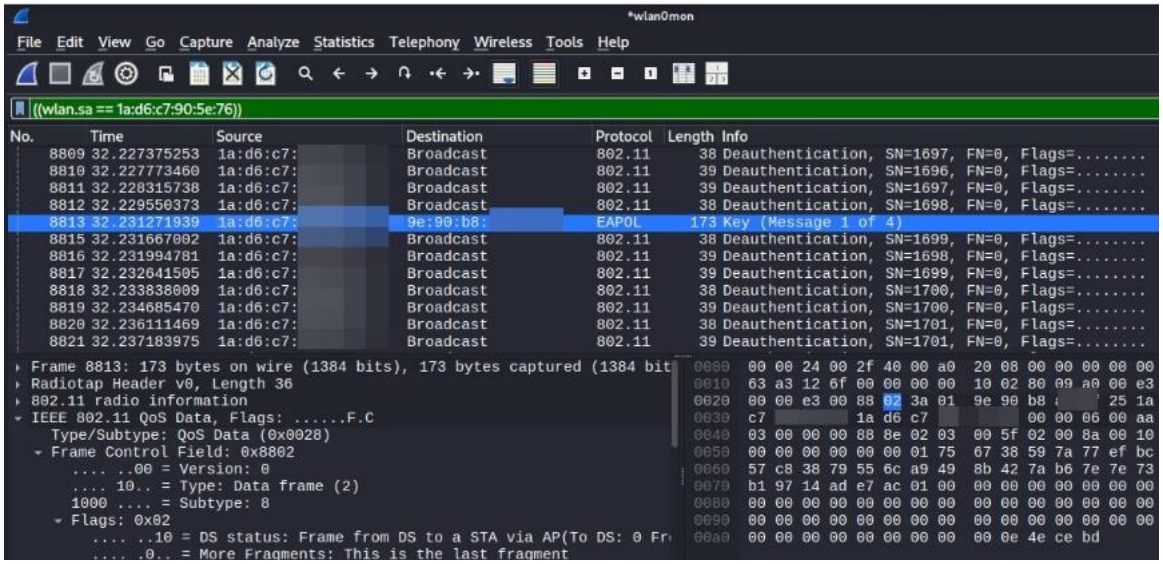
Ketiga, WPA3 menggunakan *negotiated* PMF yang berarti PMF bersifat *mandatory* dan tidak dapat di-*downgrade*. Berbeda dengan WPA2 di mana PMF bersifat *optional*, pada WPA3-SAE, *client* dan *access point* wajib menyepakati penggunaan PMF selama fase *association*. Hal ini mencegah *adversary* melakukan *downgrade attack* dengan memaksa komunikasi tanpa PMF [4], [18]. Mekanisme ini memastikan bahwa seluruh *management frame* selama sesi koneksi berlangsung telah terproteksi sejak awal, sehingga serangan berbasis *frame injection* yang tidak memiliki kredensial kriptografis yang valid akan ditolak sebelum mencapai proses manajemen jaringan.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

Dengan demikian, kegagalan serangan *deauthentication* pada WPA3 bukan hanya karena adanya "proteksi tambahan", tetapi merupakan hasil dari arsitektur keamanan berlapis yang mengintegrasikan autentikasi kriptografis, verifikasi integritas, dan proteksi *replay* pada setiap *management frame*, menjadikan manipulasi *management frame* secara fundamental tidak feasible tanpa akses terhadap kunci sesi yang valid.

4.3. *Analisis serangan brute-force WPA2 PSK, WPA3 SAE*

Pada pengujian WPA2, serangan *brute- force* dapat dilakukan setelah diperoleh rekaman autentikasi antara *client* dan *access point* akibat serangan *deauthentication*. Rekaman tersebut memuat informasi yang diperlukan dalam proses autentikasi sehingga memungkinkan dilakukan pengujian kata sandi secara *offline*. Kondisi ini menunjukkan bahwa ketika material autentikasi berhasil diperoleh, risiko serangan lanjutan menjadi terbuka meskipun prosesnya tidak terjadi secara langsung pada jaringan yang aktif. Hasil rekaman autentikasi yang memungkinkan serangan ini ditunjukkan pada Gambar 5.



Gambar 5. Penangkapan 4-way Handshake (EAPOL) pada Jaringan WPA2-PSK menggunakan Airodump-ng

Hasil percobaan menunjukkan bahwa serangan *deauthentication* dapat memicu proses koneksi ulang klien, sehingga pada kondisi tersebut *handshake* atau paket EAPOL dapat terekam. Keberadaan rekaman ini menunjukkan adanya potensi risiko lanjutan pada jaringan, karena material autentikasi dapat dimanfaatkan dalam pengujian keamanan kata sandi.

Setelah rekaman *handshake* diperoleh, tahap selanjutnya adalah melakukan simulasi serangan *brute-force* terhadap jaringan WPA2-PSK. Proses ini dilakukan secara *offline* menggunakan *wordlist* untuk menguji kemungkinan kecocokan kata sandi. Pengujian ini bertujuan untuk menilai tingkat kekuatan kata sandi yang digunakan pada jaringan tersebut. Hasil proses *brute-force attack* terhadap jaringan WPA2-PSK tersebut ditunjukkan pada Gambar 6.

p-ISSN : 2803-1507 e-ISSN : 2803-1531



Gambar 6. Proses Brute-Force Attack terhadap WPA2-PSK menggunakan Aircrack-ng dengan Wordlist 300.000 entri

Pengujian *brute-force* dilakukan sebagai tahap lanjutan setelah diperolehnya material autentikasi pada jaringan WPA2-PSK. Pada pengujian ini digunakan *wordlist* berisi sekitar 300 ribu *entri* dengan waktu eksekusi kurang lebih 2 menit. Hasil pengujian menunjukkan bahwa kata sandi yang digunakan tidak berhasil diperoleh. Meskipun demikian, tahapan ini memperlihatkan bahwa selama *handshake* dapat ditangkap, proses *brute-force* tetap dapat dilakukan, sehingga risiko serangan sangat dipengaruhi oleh kekuatan kata sandi yang digunakan.

Berbeda dengan WPA2-PSK, pengujian pada jaringan yang menggunakan protokol WPA3-SAE menunjukkan bahwa tahapan *brute-force* tidak dapat dilanjutkan. Mekanisme *Protected Management Frames* (PMF) mencegah pemutusan koneksi secara paksa, sehingga *handshake* tidak dapat diperoleh sebagai prasyarat serangan lanjutan. Dengan demikian, WPA3-SAE menunjukkan peningkatan ketahanan terhadap serangan *brute-force* dengan menutup celah yang masih dapat dimanfaatkan pada protokol WPA2-PSK.

4.4. *Analisis Hasil Uji*

Berdasarkan hasil dari *experiment* penyerangan *brute-force* dan *deauthentication* menunjukkan adanya perbedaan ketahanan atas penyerangan, beberapa variabel yang bisa menjadi perbandingan dari kedua protokol yang diuji berdasarkan perlakuan yang sama, oleh karena itu didapatkan hasil data berdasarkan pengujian diatas yang ditunjukkan pada Tabel 1.

Tabel 1. Perbandingan hasil Pengujian Serangan terhadap Protokol WPA2-PSK dan WPA3-SAE

No.	Tahap Serangan	Variable Uji	Protokol	
			WPA2-PSK	WPA3-SAE
1.	Mendapatkan informasi *access point*	MAC address, Chiper, *Channel, Auth system,* Name *access point*	Berhasil	Berhasil
2.	*Deauthentication Attack*	MAC address, *Channel*	Berhasil	Tidak Berhasil
3.	Mendapatkan *Handshake access point*	*Auth system*	Berhasil	Tidak Berhasil
4.	*Brute-force Attack*	*Handshake valid,* proses *Cracking Aircrack-ng*	Berhasil	Tidak Berhasil

Berdasarkan hasil pengujian yang dirangkum pada Table 1, terlihat adanya perbedaan ketahanan yang signifikan antara protokol WPA2-PSK dan WPA3-SAE terhadap serangan *deauthentication* dan *brute-force*. Pada tahap awal, kedua protokol masih memungkinkan proses pengumpulan informasi *access point*, seperti *MAC address* dan *channel*, yang merupakan karakteristik umum dari jaringan WLAN. Perbedaan utama mulai terlihat pada tahap *deauthentication*. Pada WPA2-PSK, serangan *deauthentication* berhasil dilakukan

p-ISSN : 2803-1507 e-ISSN : 2803-1531

sehingga memicu pemutusan koneksi klien dan memungkinkan diperolehnya *handshake*. Sebaliknya, pada WPA3-SAE, serangan ini tidak berhasil karena mekanisme *Protected Management Frames* (PMF) mencegah pemrosesan *frame manajemen* yang tidak terautentikasi. Kondisi ini secara langsung menghambat tahapan lanjutan dari serangan.

Keberhasilan memperoleh *handshake* pada WPA2-PSK memungkinkan dilakukannya serangan *brute-force* sebagai risiko lanjutan, meskipun keberhasilannya tetap bergantung pada kekuatan kata sandi yang digunakan. Sementara itu, pada WPA3-SAE, ketidakmampuan memperoleh *handshake* menyebabkan serangan *brute-force* tidak dapat dilanjutkan. Hal ini menunjukkan bahwa peningkatan keamanan pada WPA3-SAE tidak hanya bergantung pada mekanisme autentikasi, tetapi juga pada perlindungan terhadap tahapan awal serangan.

Perbedaan fundamental ini dapat dijelaskan dari *perspektif* arsitektur protokol. Pada WPA2-PSK, *management frame* seperti *deauthentication* dan *disassociation* tidak dilindungi secara kriptografis karena PMF bersifat *optional* dan sering tidak diaktifkan. Akibatnya, *access point* tidak memiliki mekanisme untuk membedakan antara *management frame* yang sah (berasal dari *client* terautentikasi) dengan *frame* palsu hasil spoofing (dengan alamat MAC yang dipalsukan). Protokol hanya memeriksa *format frame* dan alamat MAC tanpa verifikasi kriptografis, sehingga *frame* palsu yang memiliki struktur valid akan diproses sebagai *frame* yang sah [19], [20].

Sebaliknya, pada WPA3-SAE, setiap *management frame* robust harus melalui tiga tahap verifikasi protokol: (1) verifikasi kriptografis menggunakan *Message Integrity Check* (MIC) yang dihitung dari kunci sesi, (2) verifikasi *sequence counter* untuk mencegah *replay attack*, dan (3) verifikasi *association state* untuk memastikan *frame* berasal dari sesi yang valid. Ketika *deauthentication frame* hasil injeksi diterima, *access point* WPA3 mendeteksi ketiadaan MIC yang valid atau ketidaksesuaian dengan kunci sesi aktif, sehingga *frame* ditolak pada tahap validasi protokol sebelum diproses oleh *state machine* manajemen koneksi [4], [18], [19]. Mekanisme ini secara fundamental berbeda dengan WPA2, di mana tidak ada tahap verifikasi kriptografis sehingga *frame* palsu dapat langsung diproses.

Implikasi dari perbedaan arsitektural ini adalah bahwa serangan *deauthentication* pada WPA3 tidak hanya "lebih sulit" tetapi secara teoretis tidak feasible tanpa kompromi terhadap kunci sesi. Penyerang perlu memperoleh *Pairwise Master Key* (PMK) atau kunci turunannya untuk dapat membuat MIC yang valid, yang memerlukan *cryptanalytic attack* terhadap SAE *handshake* atau kompromi terhadap *endpoint*. Hal ini mengubah *threat* model dari *passive eavesdropping* dan *active frame injection* (yang feasible pada WPA2) menjadi serangan yang memerlukan *cryptographic break* atau *endpoint compromise* (yang secara komputasi tidak feasible dengan *resource moderate*).

4.5. *Implikasi Keamanan Protokol Nirkabel pada Sistem Informasi Modern*

Berdasarkan hasil dari pengujian yang dilakukan menunjukkan bahwa keamanan pada jaringan WLAN tidak bisa lagi dianggap sebagai bagian pelengkap dalam sistem informasi modern. Pada pengujian menggunakan WPA2-PSK, masih terdapat celah pada *manajemen frame* koneksi yang memungkinkan munculnya potensi serangan lanjutan, meskipun sistem sudah menggunakan mekanisme enkripsi untuk melindungi data. Kondisi ini memperlihatkan bahwa perlindungan data saja belum cukup apabila proses akses jaringan masih memiliki kelemahan.

Temuan tersebut memberikan gambaran bahwa keamanan sistem informasi modern sangat dipengaruhi oleh bagaimana jaringan dikelola sejak tahap awal koneksi. Ketika mekanisme perlindungan pada lapisan jaringan tidak berjalan dengan baik, maka risiko keamanan dapat muncul sebelum sistem benar-benar digunakan. Sebaliknya, penggunaan WPA3-SAE dengan dukungan *Protected Management Frames* (PMF) mampu menekan risiko tersebut karena proses koneksi menjadi lebih terlindungi. Dengan demikian, hasil penelitian ini menunjukkan bahwa perhatian terhadap keamanan jaringan nirkabel menjadi hal penting dalam mendukung keandalan sistem informasi modern.

Dari *perspektif* keamanan sistem informasi, temuan penelitian ini menggaris bawahi prinsip *security-by-design versus security-by-retrofit*. WPA2, meskipun memiliki enkripsi data yang kuat melalui AES-CCMP, dirancang dengan asumsi bahwa *management frame* tidak memerlukan proteksi kriptografis karena dianggap bukan bagian dari data *plane*. Asumsi desain ini terbukti keliru dalam konteks *threat landscape* modern di mana *adversary* dapat memanipulasi *control plane* (melalui *management frame*) untuk mengkompromikan data *plane*. Penambahan PMF pada WPA2 (melalui IEEE 802.11w) merupakan retrofit yang bersifat

p-ISSN : 2803-1507 e-ISSN : 2803-1531

optional, sehingga tidak mengubah *default security posture* dan bergantung pada konfigurasi administrator [4], [19].

Sebaliknya, WPA3 mengadopsi *security-by-design* dengan menjadikan PMF sebagai *mandatory requirement* dan mengintegrasikannya dengan SAE *handshake* yang menghasilkan kunci turunan untuk proteksi *management frame*. Pendekatan ini mencerminkan prinsip *defense-in-depth* di mana keamanan tidak hanya bergantung pada enkripsi data, tetapi juga pada proteksi terhadap *control plane*, *authentication mechanism*, dan *key management*. Dalam konteks *information security framework* seperti ISO 27001 atau NIST *Cybersecurity Framework*, hal ini sejalan dengan *control objective* untuk "proteksi informasi dalam transmisi" yang mencakup tidak hanya data *confidentiality* tetapi juga *control channel integrity* [4], [18].

Temuan ini memiliki implikasi praktis terhadap *wireless security governance* di organisasi modern. Pertama, kebijakan keamanan jaringan tidak boleh lagi memandang protokol keamanan *Wi-Fi* sebagai *binary choice* (aman vs tidak aman), tetapi harus mempertimbangkan *threat* model spesifik dan *attack surface* yang dihadapi. Untuk jaringan dengan *high-value asset* atau *sensitive* data, WPA2 tanpa PMF tidak lagi memenuhi *baseline security requirement* karena rentan terhadap serangan yang tidak memerlukan *sophisticated capability*. Kedua, proses *security assessment* dan *penetration testing* harus mencakup evaluasi terhadap *management plane security*, bukan hanya data *plane encryption*. Ketiga, *decision support system* (DSS) untuk pemilihan teknologi keamanan jaringan perlu mengintegrasikan evaluasi risiko berbasis *attack vector aktual*, bukan hanya *compliance requirement* atau vendor *recommendation*.

Dengan demikian, penelitian ini berkontribusi pada pengembangan *evidence-based security policy* yang mendasarkan keputusan teknologi pada validasi empiris terhadap *real-world threat*, mendukung evolusi dari *compliance-driven security* menuju *risk-based security management* dalam tata kelola keamanan informasi organisasi modern.

5. DISKUSI

Hasil pengujian menunjukkan bahwa protokol WPA2-PSK masih memproses *management frame* tanpa mekanisme verifikasi kriptografis yang memadai, sehingga pemutusan koneksi klien dapat dipicu melalui injeksi *deauthentication frame* palsu. Respons *access point* terhadap frame tersebut mengindikasikan bahwa lapisan kontrol koneksi masih bergantung pada validitas struktur frame dan alamat MAC, bukan pada autentikasi berbasis kunci sesi. Kondisi ini memperlihatkan bahwa keamanan WPA2 lebih berfokus pada perlindungan *data plane*, sementara *control plane* tetap dapat dimanipulasi. Pola ini selaras dengan temuan [19] yang menunjukkan bahwa WPA2 tanpa *Protected Management Frames* masih rentan terhadap manipulasi *management frame*.

Perilaku yang berbeda diamati pada protokol WPA3-SAE ketika dikenai skenario serangan yang sama. Mekanisme *Protected Management Frames* yang bersifat *mandatory* menyebabkan setiap *management frame* harus melalui verifikasi integritas dan autentikasi kriptografis sebelum diproses oleh *access point*. Frame yang tidak memiliki *Message Integrity Check* (MIC) yang valid ditolak pada tahap awal validasi protokol, sehingga tidak berdampak pada status koneksi klien. Temuan ini memperkuat hasil penelitian sebelumnya yang menyatakan bahwa WPA3 tidak rentan terhadap *deauthentication attack* konvensional karena perlindungan menyeluruh pada *control plane* jaringan [18].

Keberhasilan serangan *deauthentication* pada WPA2-PSK membuka peluang serangan lanjutan melalui penangkapan *4-way handshake*, yang kemudian dapat digunakan dalam skenario *offline dictionary attack*. Meskipun kata sandi tidak berhasil diperoleh dari *wordlist* yang digunakan, proses pengujian menunjukkan bahwa mekanisme serangan tetap dapat dieksekusi secara penuh ketika material autentikasi tersedia. Hal ini menegaskan bahwa risiko utama pada WPA2 tidak hanya bergantung pada keberhasilan pemecahan kata sandi, tetapi pada eksposur *handshake* itu sendiri. Temuan ini konsisten dengan penelitian Wang *et al.* serta Shamsudin dan Zolkipli yang menekankan bahwa keamanan WPA2 sangat dipengaruhi oleh kekuatan kata sandi setelah *handshake* berhasil direkam [15].

Sebaliknya, pada WPA3-SAE, kegagalan serangan *deauthentication* menghambat proses penangkapan *handshake*, sehingga serangan *brute-force* tidak dapat dilanjutkan. Ketahanan ini tidak hanya berasal dari mekanisme *Simultaneous Authentication of Equals* (SAE), tetapi juga dari integrasi SAE dengan proteksi *management frame* yang menutup tahapan awal serangan. Arsitektur ini mengubah *threat model* dari serangan berbasis *frame injection* menjadi serangan yang memerlukan kompromi kriptografis atau *endpoint*. Hasil ini sejalan dengan temuan sebelumnya yang menyatakan bahwa WPA3 menghadirkan peningkatan

p-ISSN : 2803-1507 e-ISSN : 2803-1531

keamanan yang bersifat struktural pada tingkat protokol, bukan sekadar peningkatan fitur dibandingkan WPA2 [4], [23].

6. KESIMPULAN DAN SARAN

6.1. *Kesimpulan*

Berdasarkan hasil penelitian evaluasi keamanan protokol WPA2-PSK dan WPA3-SAE terhadap serangan *deauthentication* dan *brute-force* menggunakan *aircrack-ng suite*, dapat disimpulkan beberapa hal penting sebagai berikut:

Pertama, protokol WPA2-PSK menunjukkan kerentanan signifikan terhadap serangan *deauthentication*. Hasil pengujian membuktikan bahwa *frame deauthentication* palsu dapat berhasil diinjeksikan ke *access point* dengan BSSID 1A:D6:C7:XX:XX:XX, menyebabkan pemutusan koneksi klien (MAC address 9E:90:B8:XX:XX:XX) dari jaringan. Analisis menggunakan *wireshark* menunjukkan bahwa *access point* menerima dan memproses paket *deauthentication* tanpa verifikasi autentikasi yang memadai, mengakibatkan pesan *disassociate* yang menandakan keberhasilan serangan. Hal ini mengonfirmasi bahwa WPA2-PSK tidak memiliki mekanisme proteksi yang efektif terhadap serangan *management frame manipulation*.

Kedua, protokol WPA3-SAE menunjukkan ketahanan yang jauh lebih baik terhadap serangan *deauthentication* dibandingkan WPA2-PSK. Pengujian terhadap *access point* WPA3 dengan MAC address C2:07:7A:XX:XX:XX dan klien dengan MAC address 00:C3:0A:XX:XX:XX membuktikan bahwa mekanisme *protected management frames* (PMF) yang diwajibkan pada WPA3 berhasil menolak *frame deauthentication* palsu. Meskipun *frame deauth* berhasil dikirimkan dan tereksekusi, *access point* WPA3 tidak memutuskan koneksi klien karena mampu mengidentifikasi dan memfilter *frame* yang tidak memiliki autentikasi yang valid. Temuan ini memvalidasi efektivitas PMF sebagai *countermeasure* terhadap serangan *deauthentication*.

Ketiga, dalam konteks serangan *brute-force*, protokol WPA2-PSK terbukti rentan terhadap serangan *dictionary attack* setelah *handshake* berhasil ditangkap. Proses penangkapan eapol *handshake* melalui serangan *deauthentication* dan *reconnection* klien berjalan dengan sukses, memungkinkan penyerang memperoleh data yang diperlukan untuk melakukan *password cracking*. Pengujian menggunakan *aircrack-ng* dengan *wordlist* berisi 300.000 kata menunjukkan bahwa proses *brute-force* dapat dieksekusi dengan sempurna dalam waktu 2 menit 21 detik. Meskipun dalam pengujian ini *password* "bandung764" tidak ditemukan dalam *wordlist* yang digunakan, hal ini menunjukkan bahwa keberhasilan serangan sangat bergantung pada kompleksitas *password* dan kelengkapan *dictionary* yang digunakan. Secara teknis, mekanisme serangan *brute-force* terhadap WPA2-PSK terbukti *feasible* dan efektif.

Keempat, protokol WPA3-SAE menunjukkan resistensi penuh terhadap serangan *brute-force* berbasis *dictionary attack* yang umum digunakan pada WPA2. Kegagalan dalam tahap penangkapan *handshake* akibat efektivitas PMF mengakibatkan serangan *brute-force* tidak dapat dilanjutkan. Berbeda dengan WPA2 yang menggunakan *4-way handshake* dengan PSK (*Pre Shared Key*), WPA3 mengimplementasikan *simultaneous authentication of equals* (SAE) atau *dragonfly handshake* yang tidak mengirimkan informasi *password* dalam bentuk yang dapat ditangkap untuk *offline dictionary attack*. Mekanisme SAE yang berbasis *Diffie-Hellman key exchange* menghasilkan kunci sesi yang unik untuk setiap koneksi, sehingga jika *handshake* berhasil ditangkap, penyerang tidak dapat melakukan *offline brute-force* seperti pada WPA2. Temuan ini mengonfirmasi bahwa WPA3-SAE secara arsitektural lebih aman terhadap serangan *dictionary* dan *brute-force*.

Kelima, perbandingan komprehensif menunjukkan bahwa WPA3-SAE memberikan peningkatan keamanan yang substansial dibandingkan WPA2-PSK. Dari empat tahapan pengujian yang dilakukan (mendapatkan informasi *access point*, *deauthentication attack*, mendapatkan *handshake*, dan *brute-force*), WPA2-PSK berhasil ditembus pada seluruh tahapan, sementara WPA3-SAE hanya rentan pada tahap pengumpulan informasi *access point* yang bersifat pasif. Pada tiga tahapan serangan aktif (*deauthentication*, *handshake capture*, dan *brute-force*), WPA3-SAE menunjukkan ketahanan penuh. Hal ini membuktikan bahwa implementasi PMF dan SAE pada WPA3 secara signifikan meningkatkan *resilience* jaringan *wireless* terhadap serangan yang umum digunakan untuk mengeksploitasi WPA2.

Dengan demikian, penelitian ini menjawab pertanyaan penelitian bahwa WPA3-SAE jauh lebih efektif dibandingkan WPA2-PSK dalam mencegah serangan *deauthentication* dan *brute-force*, dengan PMF sebagai

p-ISSN : 2803-1507 e-ISSN : 2803-1531

factor kunci yang memberikan proteksi terhadap *manipulation frame* dan SAE sebagai mekanisme yang mengeliminasi kerentanan terhadap *offline dictionary attack*.

6.2. *Saran*

Berdasarkan hasil penelitian dan keterbatasan yang ditemukan, beberapa saran dapat direkomendasikan untuk penelitian selanjutnya, praktisi keamanan jaringan, dan pembuat kebijakan:

6.2.1. *Saran untuk Penelitian Lanjutan*

1. Pengujian terhadap Serangan *Advanced*
   Penelitian selanjutnya disarankan untuk menguji efektivitas WPA3-SAE terhadap serangan yang lebih canggih seperti *side-channel attacks*, *downgrade attacks* pada *transition mode* WPA2/WPA3, dan *evil twin attacks* menggunakan *captive portal*. Penelitian ini hanya menguji serangan *deauthentication* dan *brute-force* konvensional, sehingga evaluasi terhadap *attack vectors* yang lebih *sophisticated* diperlukan untuk memberikan gambaran komprehensif tentang ketahanan WPA3 dalam *real world scenarios*.
2. Pengujian dengan Variasi *Tools*
   Meskipun *aircrack-ng* merupakan *tools* yang *widely-adopted* untuk *wireless penetration testing*, penelitian mendatang dapat menggunakan *tools* lain seperti *hashcat*, *wifite*, atau *tools* khusus untuk WPA3 seperti *Dragonblood attack tools* untuk memberikan perspektif yang lebih luas tentang *vulnerabilities* yang mungkin ada.
3. Analisis Performa dan *Overhead*
   Penelitian selanjutnya perlu mengukur dampak implementasi PMF dan SAE terhadap performa jaringan, termasuk *latency*, *throughput*, dan *connection establishment time*. Hal ini penting untuk mengevaluasi *trade-off* antara *security enhancement* dan *network performance*, terutama dalam konteks *high-density environments* atau *IoT deployments*.
4. Pengujian pada Implementasi berbeda
   Penelitian ini menggunakan *access point* dengan *vendor* dan implementasi tertentu (TP-LINK untuk WPA2 dan OPPO untuk WPA3). Studi komparatif terhadap berbagai vendor dan implementasi WPA3 (*enterprise-grade access points*, *consumer routers*, *mobile hotspots*) diperlukan untuk mengidentifikasi *potential implementation specific vulnerabilities*.
5. Evaluasi *Dictionary Size* dan *Password Complexity*
   Penelitian lanjutan disarankan untuk menggunakan variasi ukuran *wordlist* (dari *small wordlist* hingga *large-scale dictionaries* seperti *Rock You* atau *HavelBeenPwned*) dan melakukan analisis statistik tentang korelasi antara *password complexity*, *wordlist size*, dan *success rate* serangan *brute-force* terhadap WPA2.

6.2.2. *Saran untuk Praktisi Keamanan dan Administrator Jaringan*

1. Migrasi ke WPA3
   Administrator jaringan sangat disarankan untuk melakukan migrasi dari WPA2 ke WPA3 sesegera mungkin, mengingat kerentanan signifikan WPA2 terhadap serangan *deauthentication* dan *brute-force* yang telah terbukti dalam penelitian ini. Meskipun WPA3 *adoption rate* masih rendah secara global, *security benefits* yang ditawarkan jauh lebih besar dibandingkan *compatibility concerns*.
2. Implementasi *Strong Password Policy*
   Untuk jaringan yang masih menggunakan WPA2 karena *compatibility requirements*, implementasi kebijakan *password* yang kuat menjadi sangat kritikal. *Password* harus memiliki minimal 12-16 karakter dengan kombinasi *uppercase*, *lowercase*, *numbers*, dan *special characters*, serta tidak menggunakan kata yang ada dalam *common dictionaries*. Penelitian ini menunjukkan bahwa *password* "bandung764" yang relatif sederhana dapat menjadi target *brute-force* yang *feasible*.
3. Enable PMF pada WPA2
   Meskipun PMF bersifat opsional pada WPA2, administrator sangat disarankan untuk mengaktifkannya secara *mandatory* (*required*) bukan *optional* untuk mengurangi risiko *deauthentication attacks*, terutama pada jaringan *enterprise* atau *public hotspots* yang berisiko tinggi.
4. Hindari *Transition Mode*
   Untuk organisasi yang telah melakukan *upgrade* ke WPA3, disarankan untuk tidak menggunakan *transition mode* (WPA2/WPA3 *mixed mode*) kecuali benar-benar diperlukan, karena dapat

p-ISSN : 2803-1507 e-ISSN : 2803-1531

membuka celah untuk *downgrade attacks*. Jika *transition mode* diperlukan, implementasikan *network segmentation* dengan VLAN berbeda untuk WPA2 dan WPA3 *clients*.

5. Regular *Security Auditing*
   Lakukan *penetration testing* berkala terhadap infrastruktur *wireless* menggunakan metodologi yang serupa dengan penelitian ini untuk mengidentifikasi *potential vulnerabilities* dan memvalidasi efektivitas *security controls* yang telah diimplementasikan.
6. *Monitoring* dan *Detection*
   Implementasikan *wireless intrusion detection systems* (WIDS) atau *wireless intrusion prevention systems* (WIPS) yang dapat mendeteksi anomali seperti *excessive deauthentication frames*, *rogue access point*, dan *suspicious authentication attempts* untuk memberikan *early warning* terhadap *potential attacks*.

6.2.3. *Saran untuk Pembuat Kebijakan dan Standardisasi*

1. *Mandatory WPA3 for Public Network*
   Pembuat kebijakan publik dan regulator telekomunikasi disarankan untuk membuat regulasi yang mewajibkan penggunaan WPA3 minimal untuk *public hotspots*, *institutional networks* (pendidikan, kesehatan, pemerintahan), dan *critical infrastructure*, mengingat *severe vulnerabilities* WPA2 yang telah dibuktikan.
2. *Awareness Campaign*
   Diperlukan kampanye edukasi kepada masyarakat umum dan *IT professionals* tentang pentingnya *upgrading* ke WPA3 dan risiko keamanan yang terkait dengan *continued use of* WPA2, terutama di indonesia dimana WPA3 *adoption* masih sangat rendah.
3. *Vendor Compliance*
   Mendorong *vendor* perangkat *wireless* untuk mempercepat implementasi WPA3 *certification* dan *backward compatibility support*, serta menyediakan *firmware updates* untuk *legacy devices* yang memungkinkan untuk di *upgrade* ke WPA3 *support*.

6.2.4. *Keterbatasan Penelitian*

Penelitian ini memiliki beberapa keterbatasan yang perlu dipertimbangkan:

1. *Limited Test Environment*
   Pengujian dilakukan dalam *controlled lab environment* dengan jumlah *access points* dan *clients* yang terbatas. *Real world scenarios* dengan *network density* yang tinggi, *interference*, dan *multiple concurrent users* mungkin menghasilkan hasil yang berbeda.
2. *Single Wordlist Testing*
   Pengujian *brute-force* hanya menggunakan satu *wordlist* dengan 300.000 kata. Penggunaan *wordlist* yang lebih besar atau *targeted wordlist* yang disesuaikan dengan *demographic profile* target mungkin menghasilkan *success rate* yang berbeda.
3. *Vendor-Specific Implementation*
   Hasil penelitian mungkin bervariasi tergantung pada *vendor* dan *firmware version* dari *access points* yang digunakan, mengingat implementasi standar dapat berbeda antar *vendor*.
4. *Absence of Advanced Attack Testing*
   Penelitian ini tidak menguji *attack vectors* yang lebih *sophisticated* seperti KRACK (*Key Reinstallation Attack*), *Dragonblood attacks*, atau *exploitation of specific implementation flaws* yang mungkin ada pada *certain vendors*.

Meskipun demikian, penelitian ini memberikan kontribusi signifikan dalam memvalidasi efektivitas WPA3-SAE terhadap *common attack vectors* yang sering digunakan untuk mengeksploitasi *wireless networks*, dan memberikan *evidence-based recommendations* untuk *security practitioners* dan *policymakers* dalam konteks *wireless network security* di Indonesia.

DAFTAR PUSTAKA

[1] A. Oktavia dan A. Wibowo, "A New Theoretical Framework for Analyzing the Social and Economic Impacts of Artifical Intelligence Within the Digital Economy," *Journal of Management and Informatics*, vol. 4, no. 2, pp. 859–871, Agu 2025, doi: 10.51903/jmi.v4i2.156.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

[2] W. A. Kuncoro dan L. Santoso, "Kemacetan Jaringan Akibat Media Sosial: Menganalisis Dampaknya terhadap Efisiensi Transmisi Data Nirkabel," *Jurnal Ilmiah Sistem Informasi*, vol. 4, no. 2, pp. 130–141, Mei 2025, doi: 10.51903/jt9z2f09.

[3] B. Hartono, F. D. Silalahi, dan M. Muthohir, "Transformers in Cybersecurity: Advancing Threat Detection and Response through Machine Learning Architectures," *Journal of Technology Informatics and Engineering*, vol. 3, no. 3, pp. 382–396, Des 2024, doi: 10.51903/jtie.v3i3.211.

[4] Department of Electrical Engineering, University of Mosul, Mosul, Iraq, A. A. Ghanim, dan M. Y. Thanoun, "Evaluating the Effectiveness of WPA3 Protocol against Advanced Hacking Attacks," *IJWMT*, vol. 15, no. 4, pp. 1–18, Agu 2025, doi: 10.5815/ijwmt.2025.04.01.

[5] T. A. Kurniawan, "Analisa Keamanan Jaringan Wifi Terhadap Serangan Packet Sniffing," *Jurnal Ilmiah Fakultas Teknik LIMIT'S*, vol. 16, no. 2, pp. 11–15, 2020. [Online]. Available: https://teknik.usni.ac.id/jurnal/2.%20t.adi.pdf

[6] R. S. Pratikno, C. Trinata, dan G. B. Hertantyo, "Kajian Literatur Analisis Keamanan Jaringan," Pendas: *Jurnal Ilmiah Pendidikan Dasar*, vol. 10, no. 2, pp. 361–370, 2025, doi:10.23969/jp.v10i02.28330.

[7] A. Halbouni, L.-Y. Ong, dan M.-C. Leow, "Wireless Security Protocols WPA3: A Systematic Literature Review," IEEE Access, vol. 11, pp. 112438–112450, 2023, doi:10.1109/access.2023.3322931.

[8] K. A. Adbeib, "Comprehensive Study on Wi-Fi Security Protocols by Analyzing WEP, WPA, and WPA2," *African Journal of Advanced Pure and Applied Sciences (AJAPAS)*, vol. 2, no. 4, pp. 385–402, Dec. 2023, doi:10.65418/ajapas.v2i4.659.

[9] D. T. Zaidan, "Analyzing Attacking Methods on Wi-Fi Wireless Networks Pertaining (WEP, WPA-WPA2) Security Protocols," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 9, no. 4, pp. 1093–1101, 2021, doi:10.21533/pen.v9.i4.1011.

[10] A. B. Nuhaenibudi As-sajid dan R. E. Putra, "Analisis dan Pengujian Dictionary Attack terhadap WPA3 Berbasis Script," *JINACS*, vol. 5, no. 02, pp. 216–222, Sep 2023, doi: 10.26740/jinacs.v5n02.p216-222.

[11] M. D. P. Dar, R. Lorch, A. Sadeghi, V. Sorcigli, H. Gollier, C. Tinelli, M. Vanhoef, dan O. Chowdhury, "SAECRED: A State-Aware, Over-The-Air Protocol Testing Approach for Discovering Parsing Bugs in SAE Handshake Implementations of COTS Wi-Fi Access Points," in *Proc. IEEE Symposium on Security and Privacy (S&P)*, San Francisco, CA, USA, May 2025, pp. 3691–3709, doi:10.1109/sp61157.2025.00211.

[12] Y. Mulyanto, H. Herfandi, dan R. Candra Kirana, "Analisis Keamanan Wireless Local Area Network (WLAN) terhadap Serangan Brute Force dengan Metode Penetration Testing (Studi Kasus: RS H.Lmanambai Abdulkadir)," *JINTEKS*, vol. 4, no. 1, pp. 26–35, Feb 2022, doi: 10.51401/jinteks.v4i1.1528.

[13] A. Z. Ifani, N. F. Aspar, A. D. Setiawan, dan M. Azlam, "Pengujian Keamanan Sistem Informasi Data Kependudukan Menggunakan Metode Pentetration Testing," *Jurnal Fokus Elektroda: Energi Listrik, Telekomunikasi, Komputer, Elektronika dan Kendali*, vol. 9, no. 2, pp. 73–78, 2024. [Online]. Available: https://id.scribd.com/document/810765900/pengujian-keamanan-sistem-informasi-data-kependudukan-menggunakan-metode-pentetration-testing

[14] H. S. Harahap, A. A. Rahman, I. Suraswati, dan S. N. Neyman, "Memahami Cara Kerja Phishing Menggunakan Tools Pada Kali Linux," *Journal of Internet and Software Engineering*, vol. 1, no. 2, pp. 1–11, Jun. 2024. [Online]. Available: https://journal.pubmedia.id/index.php/pjise/article/view/2723

[15] M. A. N. Shamsudin dan M. F. Zolkipli, "A Case Study of Wi-Fi Penetration Testing: WPA2WPA3 Cracking," *Borneo International Journal*, vol. 8, no. 2, pp. 81–89, Jul. 2025. [Online]. Available: https://majmuah.com/journal/index.php/bij/article/view/696

[16] M. S. Ariyanto, G. B. Hertantyo, dan B. Hartati, "Serangan Deauthentication Attack Pada Wireless Access Point: Systematic Literatur Review," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 4, pp. 6606–6612, 2025, doi:10.36040/jati.v9i4.13808.

[17] Y. Mulyanto, S. S. Qanita, D. Wiryatari, dan F. Idifitriani, "Analisis Perbandingan Kinerja dan Keamanan Protokol WPA2 dan WPA3 dengan Metode Penetration Testing," *Jurnal Informatika dan Rekayasa Elektronik*, vol. 8, no. 1, pp. 140–148, 2025, doi:10.36595/jire.v8i1.1539.

[18] A. Mathew, E. Jackson, dan A. Tobesman, "Evaluating the Efficacy of WPA3 against Advanced Attacks: A Comparative Analysis with WPA2 in Real-World," *J Inform Techn Int*, vol. 3, no. 1, 2025, doi:10.33790/jiti1100105.

[19] D. Schepers, A. Ranganathan, dan M. Vanhoef, "On the Robustness of Wi-Fi Deauthentication Countermeasures," In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, San Antonio TX USA: ACM, Mei 2022, pp. 245–256. doi: 10.1145/3507657.3528548.

[20] D. Schepers, A. Ranganathan, dan M. Vanhoef, "Let Numbers Tell the Tale: Measuring Security Trends in Wi-Fi Networks and Best Practices," In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, Abu Dhabi, United Arab Emirates: ACM, Jun. 2021, pp. 100–105, doi:10.1145/3448300.3468286.

[21] M. Kaleem, M. A. Mushtaq, S. A. Ramay, A. Mahmood, T. A. Khan, S. K. Hussain, A. Anwar, dan H. A. Bhatti, "Navigating Side-Channel Attacks: A Comprehensive Overview of Cryptographic System Vulnerabilities," *Journal of Computing & Biomedical Informatics*, vol. 7, no. 2, 2024, doi:10.56979/702/2024.

[22] N. M. M. Niranjan, V. Kothamasu, dan N. Kenchaiah, "Method to Support iPSK for WPA3 Clients as Well as Reduce Online Dictionary Attacks," *Technical Disclosure Commons*, May 17, 2022. [Online]. Available: https://www.tdcommons.org/dpubs_series/5139

[23] E. Chatzoglou, G. Kambourakis, dan C. Kolias, "How Is Your Wi-Fi Connection Today? DoS Attacks on WPA3-SAE," *Journal of Information Security and Applications*, vol. 64, pp. 103058, Feb. 2022, doi:10.1016/j.jisa.2021.103058.

[24] M. Kyei dan M. Asante, "Penetration Testing of IEEE 802.11 Encryption Protocols Using Kali Linux Hacking Tools," *IJCA*, vol. 176, no. 32, pp. 26–33, Jun. 2020, doi:10.5120/ijca2020920365.

[25] J. Cathcart dan T. Khan Mohd, "Password Hacking Analysis of Kali Linux Applications," In *Intelligent Sustainable Systems*, J. S. Raj, I. Perikos, and V. E. Balas, Ed., Lecture Notes in Networks and Systems, vol. 665, Singapore: Springer Nature Singapore, 2023, pp. 815–828, doi:10.1007/978-981-99-1726-6_63.

[26] T. Ariyadi, I. Irham, dan E. F. Cahyadi, "An Evaluation of Wireless Network Security with Penetration Testing Method at PT PLN UP2D S2JB," *J. INFOTEL*, vol. 16, no. 1, Feb. 2024, doi:10.20895/infotel.v16i1.1057.

[27] K. Wang, D. Evans, P. Hui, D. Lo, dan J. Li, "Assessing Certificate Validation User Interfaces of WPA Supplicants," In *Proceedings of the 28th Annual International Conference on Mobile Computing and Networking,* Sydney, NSW, Australia: ACM, Oct. 2022, pp. 501–513, doi:10.1145/3495243.3517026.

[28] M. Xu, Y. Zhang, H. Liu, L. Ma, dan Q. Li, "Beamforming Made Malicious: Manipulating Wi-Fi Traffic via Beamforming Feedback Forgery," In *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking*, Washington, D.C., USA: ACM, Dec. 2024, pp. 908–922, doi:10.1145/3636534.3690669.

p-ISSN : 2803-1507 e-ISSN : 2803-1531

[29] K. Chadee, W. Goodridge, dan K. Khan, "Recovering WPA-3 Network Password by Bypassing the Simultaneous Authentication of Equals Handshake Using Social Engineering Captive Portal," *CoRR*, vol. abs/2412.15381, Dec. 2024. [Online]. Available: https://arxiv.org/abs/2412.15381