SERANGAN *DEAUTHENTICATION ATTACK* PADA *WIRELESS ACCESS POINT* : *SYSTEMATIC LITERATUR REVIEW*

Muhammad Saddam Ariyanto, Galuh Boy Hertantyo, Besse Hartati
Manajemen Teknologi Keimigrasian, Politeknik Imigrasi
RJHR+CQH, Jl. Satria - Sudirman, RT.001/RW.014, Tanah Tinggi,
Kec. Tangerang, Kota Tangerang, Banten 15119
saddamkeren99@gmail.com

ABSTRAK

Jaringan Wi-Fi rentan terhadap serangan siber seperti Deauthentication Attack, yang dapat memutus koneksi pengguna secara paksa dan membuka celah bagi serangan lanjutan. Penelitian ini menggunakan metode *Systematic Literature Review* (SLR) dengan pendekatan PRISMA untuk mengkaji metode, jenis pengujian, dan tools yang digunakan dalam evaluasi keamanan *Wireless Access Point* (WAP). Hasil menunjukkan bahwa *Deauthentication Attack* adalah serangan paling umum, dengan *tools* seperti *Aircrack-ng* dan *Fluxio*n paling sering digunakan. Fokus utama pengujian lebih kepada pencegahan dan perlindungan jaringan dari ancaman siber.

Kata kunci : *Deauthentication Attack, Wireless Access Point, Keamanan Jaringan, Systematic Literature Review, Aircrack-ng, Fluxion.*

1. PENDAHULUAN

Dengan meningkatnya jumlah pengguna internet di Indonesia, diperlukan pengawasan dan perlindungan sistem untuk mencegah serangan kejahatan siber. Berdasarkan laporan Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) dari Badan Siber dan Sandi Negara (BSSN), tercatat sebanyak 88.414.926 serangan siber terjadi dalam periode 1 Januari hingga 12 April 2020 [2].

Sasaran utama penyerang ini dapat mengganggu jaringan dan mencoba mencuri informasi sensitif seperti infomasi keimigrasian atau bahkan pengunaan E-Bangking pada jaringan nirkabel Umum. AP palsu mudah disebar, sulit dideteksi, dan membuka peuang terhadap jaringan akan berbagai serangan.

Keamanan WiFi lebih rentan dibandingkan jaringan kabel, karena peretas dapat mengaksesnya tanpa harus terhubung secara fisik [5]. Kurangnya kesadaran pengguna dalam menjaga keamanan jaringan membuka peluang bagi peretas untuk menyusup [6]. Seiring bertambahnya jumlah jaringan nirkabel dan sensor yang tersebar, ancaman serangan terhadap sistem ini pun semakin meningkat [7].

Teknologi nirkabel *(wireless)* telah menjadi bagian penting dalam berbagai sektor, mulai dari institusi pendidikan, perkantoran, hingga rumah tangga. Keunggulan utamanya adalah kemudahan akses dan mobilitas dalam berkomunikasi dan bertukar data. Namun, meskipun memberikan banyak kemudahan, jaringan nirkabel cenderung memiliki tingkat kerentanan yang lebih tinggi dibandingkan jaringan kabel karena sifatnya yang terbuka dan tidak memerlukan koneksi fisik [1].

Salah satu ancaman nyata terhadap jaringan nirkabel adalah serangan *Deauthentication*, yaitu teknik yang digunakan untuk memutus paksa koneksi antara klien dan *access point (AP).* Serangan ini memanfaatkan kelemahan dalam protokol manajemen *Wi-Fi* yang memungkinkan pengiriman paket deauthentication tanpa proses otentikasi [2].

Sementara itu, Lina dan Fernandes [5] mengidentifikasi bahwa perangkat murah seperti *ESP8266* juga mampu digunakan untuk melakukan serangan Deauthentication secara otomatis, menjadikan serangan ini tidak hanya berbahaya tetapi juga semakin mudah diakses oleh peretas pemula.

Melihat maraknya kasus dan kemudahan dalam pelaksanaan serangan ini, penelitian ini bertujuan untuk mengkaji secara sistematis berbagai literatur yang berkaitan dengan *Deauthentication Attack*, mulai dari metode, jenis pengujian yang dilakukan, hingga *tools* yang digunakan, dalam upaya meningkatkan keamanan jaringan *Wireless Access Point (WAP).*

Selain itu, metode ini sering dimanfaatkan sebagai langkah awal dalam pencurian data penting pengguna. Setelah koneksi jaringan *Wi-Fi* pengguna terputus, penyerang dapat membuat SSID *Wi-Fi* palsu dengan nama yang sama seperti jaringan sebelumnya untuk menipu pengguna agar terhubung. Selanjutnya, pengguna diarahkan ke halaman *login* palsu (*fake captive portal)* yang dirancang menyerupai halaman resmi. Jika pengguna tidak teliti dan memasukkan informasi seperti email, kata sandi, atau *username*, maka data tersebut dapat dicuri dan disalahgunakan oleh penyerang [8].

2. TINJAUAN PUSTAKA

Keamanan jaringan nirkabel menjadi isu krusial dalam dunia siber, terutama seiring dengan meningkatnya jumlah pengguna Wi-Fi. Jaringan nirkabel memiliki tingkat kerentanan yang lebih tinggi dibandingkan dengan jaringan kabel karena peretas dapat mengaksesnya tanpa perlu koneksi fisik [9]. Selain itu, rendahnya kesadaran pengguna dalam menjaga keamanan jaringan mereka juga menjadi faktor utama yang memungkinkan terjadinya serangan siber [10].

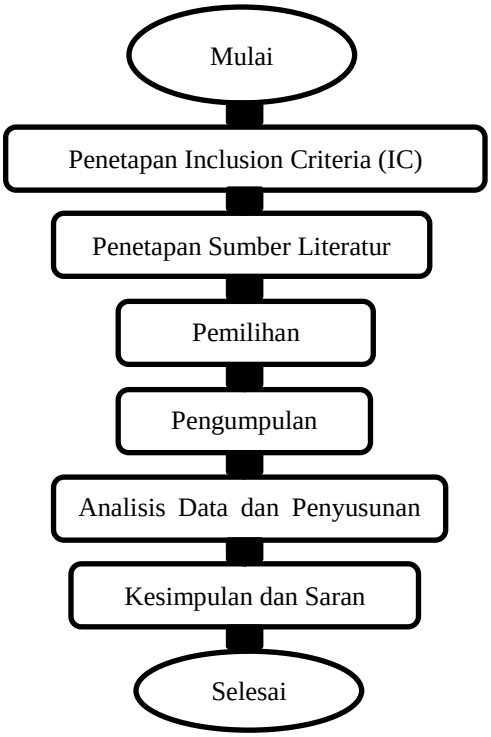
Satu metode serangan yang sering digunakan oleh peretas untuk mencuri informasi sensitif adalah Deauthentication Attack. Serangan ini bertujuan untuk mengganggu akses jaringan saat klien sedang menggunakannya. Mekanismenya dilakukan dengan cara penyerang memanfaatkan MAC address milik klien untuk mengirimkan pesan ke jaringan nirkabel, yang kemudian menyebabkan terputusnya koneksi. Dengan kata lain, penyerang mengirimkan permintaan palsu ke jaringan agar koneksi klien terputus secara paksa [12].

Salah satu alat yang sering digunakan untuk melakukan pengujian keamanan jaringan terhadap serangan Deauthentication adalah Kali Linux. Kali Linux merupakan distribusi sistem operasi berbasis Linux yang dirancang khusus untuk pengujian penetrasi dan keamanan siber [13]. Dengan berbagai alat bawaan seperti *Aircrack-ng, Wifiphisher,* dan *Ettercap,* Kali Linux memungkinkan para profesional keamanan informasi untuk mengidentifikasi serta mengevaluasi kerentanan dalam sistem jaringan. Untuk melancarkan serangan ini, peretas menggunakan berbagai alat yang tersedia di Kali Linux, yang secara khusus dikembangkan untuk pengujian keamanan dan penetrasi jaringan.

a. *Aircrack-ng*
   Aircrack-ng adalah salah satu alat paling populer dalam pengujian keamanan jaringan *Wi-Fi. Aircrack-ng* sering digunakan dalam *Evil Twin Attack* untuk menangkap handshake WPA/WPA2 serta melakukan serangan *deauthentication* terhadap pengguna jaringan asli.
b. *Fluxion*
   Fluxion adalah alat *(tool)* untuk pengujian keamanan jaringan *Wi-Fi* yang berjalan di sistem operasi berbasis Linux, termasuk Kali Linux. *Fluxion* bekerja dengan metode *Evil Twin Attack,* yaitu menciptakan jaringan *Wi-Fi* palsu yang meniru jaringan asli dengan tujuan mendapatkan kredensial pengguna (seperti kata sandi *Wi-Fi)* melalui teknik *phishing* [15].

3. METODE PENELITIAN

Penelitian ini mengimplementasikan pendekatan *Systematic Literature Review* (*SLR*) untuk menganalisis serangan *Deauthentication* pada *Wireless Access Point* (*WAP*). Penelitian dilakukan dengan mengikuti tahapan yang terstruktur, yang dimulai dari penetapan kriteria kelayakan literatur hingga pengumpulan data untuk mendapatkan hasil akhir yang relevan dengan tujuan penelitian. Adapun alur dari tahapan penelitian yang dilakukan adalah sebagai berikut:



Gambar 1. Flowchart Penel*itian*

3.1. Tahap 1: Penetapan Inclusion Criteria (IC)

a. IC1: Artikel harus merupakan penelitian asli yang ditulis dalam Bahasa Inggris atau Indonesia.
b. IC2: Artikel yang diterbitkan dalam rentang waktu antara tahun 2007 hingga 2024.
c. IC3: Artikel yang membahas tentang serangan Deauthentication pada Wireless Access Point.

3.2. Tahap 2: Penetapan Sumber Literatur

Sumber literatur dikumpulkan dari basis data yang kredibel seperti IEEE Xplore, Scopus, dan Google Scholar. Pada tahap ini, dilakukan pencarian artikel yang memenuhi kriteria kelayakan yang telah ditetapkan pada tahap sebelumnya. Artikel-artikel yang memenuhi kriteria akan dipilih untuk dianalisis lebih lanjut.

3.3. Tahap 3: Pemilihan Literatur

Pemilihan literatur dilakukan berdasarkan kata kunci yang relevan, seperti "Serangan Wireless Access Point" dan "Deauthentication pada Wireless Access Point". Setiap artikel yang ditemukan melalui pencarian kata kunci akan dianalisis judul, abstrak, dan kesesuaian konten dengan topik penelitian. Artikel yang dianggap relevan akan dipilih untuk proses tinjauan lanjutan.

3.4. Tahap 4: Pengumpulan Data

Pada tahap ini, data dikumpulkan dari artikel yang terpilih berdasarkan kriteria yang telah ditetapkan. Pengumpulan data dilakukan secara manual dengan membuat formulir ekstraksi data untuk memastikan bahwa informasi yang dikumpulkan

relevan dan sesuai dengan tujuan penelitian. Setelah melakukan penyaringan dari total 1.815.718 jurnal yang ditemukan, hanya 47 artikel yang memenuhi syarat untuk dijadikan referensi dalam penelitian ini.

3.5. Tahap 5: Analisis Data dan Penyusunan Hasil

Data yang dikumpulkan kemudian dianalisis dengan membandingkan hasil penelitian yang ada. Analisis ini melibatkan identifikasi berbagai metode serangan, jenis pengujian, serta alat yang digunakan dalam evaluasi keamanan Wireless Access Point. Hasil analisis akan digunakan untuk menarik kesimpulan mengenai keamanan jaringan Wi-Fi, serta memberikan rekomendasi terkait langkah-langkah mitigasi yang perlu diterapkan, seperti penggunaan WPA3 dan penerapan Intrusion Detection Systems (IDS).

Hasil dari penelitian ini menunjukkan bahwa serangan Deauthentication adalah metode yang paling umum digunakan untuk menyerang Wireless Access Point, terutama karena kemudahannya dalam dieksekusi dan dampaknya terhadap koneksi pengguna. Pengujian keamanan lebih sering dilakukan untuk mengidentifikasi potensi celah sebelum terjadinya serangan nyata. Tools yang sering digunakan dalam pengujian ini antara lain Aircrack-ng, Fluxion, ESP8266, dan Aireplay-ng.

Tabel 1. Hasil tinjauan literatur

Sumber	Serangan *Wireless Access Point*	*Deauthentication* Pada *Wireless Access Point*	Kandidat	Terpilih
IEEE Xplore	1.676	50	4	1
Google Scholar	1.660	608	35	20
ACM Digital Library	12.750	102	5	2
Total	16.086	760	44	23

3.6. Research Question

Tabel 2. Pertanyaan Penelitian

ID	Pertanyaan Penelitian	Latar Belakang
RQ1	Metode apa yang dilakukan untuk melakukan Analisis pada jaringan *Wireless Access Point* ?	Mengidentifikasikan Metode yang pernah dilakukan mengenai Analisis pada jaringan *Wireless Access Point ?*
RQ2	Jenis apa yang diujikan pada *Wireless Access Point ?*	Mengidentifikasikan Jenis apa yang diujikan pada *Wireless Access Point ?*
RQ3	Tools apa yang digunakan untuk menguji jaringan *Wirelss Access Point?*	Mengidentifikasikan tools apa yang digunakan untuk menguji jaringan Wirelss Access Point?

4. HASIL DAN PEMBAHASAN

4.1. Hasil Tinjauan Literatur

Tabel 3 menyajikan rangkuman dari berbagai jurnal yang ditinjau dalam penelitian ini, yang meliputi penulis, judul penelitian, tahun terbit, metode yang digunakan, jenis pengujian (apakah fokus pada keamanan atau serangan), serta tools atau alat yang digunakan dalam masing-masing penelitian. Tujuan dari tabel ini adalah untuk memperlihatkan pola dan tren penelitian terkini mengenai *Deauthentication Attack* terhadap *Wireless Access Point*.

Tabel 3. Hasil Tinjauan Literatur

NO	Penulis	Judul	Tahun	Metode	Jenis	Tools
1.	T. Pangestu, R. Liza	Analisis…[1]	2022	*DNS Spoofing*	Keamanan	*Ettercap*
2.	Satria Galang, dkk	Analisis…[2]	2023	*Peneration Testing*	Keamanan	*Aircrack-ng*
3.	L. Muhammad, Z. Fikri	Analisis…[3]	2023	*Deauther Attack*	Keamanan	*ESP8266 V3*
4.	Prasetyo, dkk	Perbandingan…[4]	2022	*Penetration Testing*	Keamanan	*Fluxion*
5.	M. Fauzan, A. Arifin	Wireless…[5]	2021	*Deauther Attack*	Serangan	*Aircrack*
6.	Kali Linux	Kali…[6]	2013	*Peneration Testing*	Keamanan	*Fluxion*
7.	D. Erisma Faishol, dkk	Analisis…[7]	2024	*Peneration Testing*	Keamanan	*Airodump-ng*
8.	M. Rahmat, T. Desyani	Implementasi…[8]	2024	*Deauther* dan *Evil Twin Attack*	Serangan	*Packet sniffer*
9.	A. Aman	Pengujian…[9]	2023	*Deauther*, *Evil Twin Attack* dan *Web Phising*	Keamanan	*Web*
10.	A. Andika Putra	Analisis…[10]	2021	*Penetration Testing*	Keamanan	*Arcai.com*
11.	Lina, Ika Mei, dkk	Analisis…[11]	2022	*Deauther* dan *Evil Twin Attack*	Serangan	*ESP8266*
12.	A.Nuhaenibudi	Analisis…[12]	2023	*Deauther* dan *Dragonblood Attack*	Serangan	*Aircrack-ng*
13.	T. Ariyadi, I. Irham,	An Evaluation…[13]	2024	*Peneration Testing*	Keamanan	*Airgedon*
14.	I. Ramadhan, H. Seta	Pengamanan…[14]	2020	*Deauther Attack*	Keamanan	*Aireplay-ng*

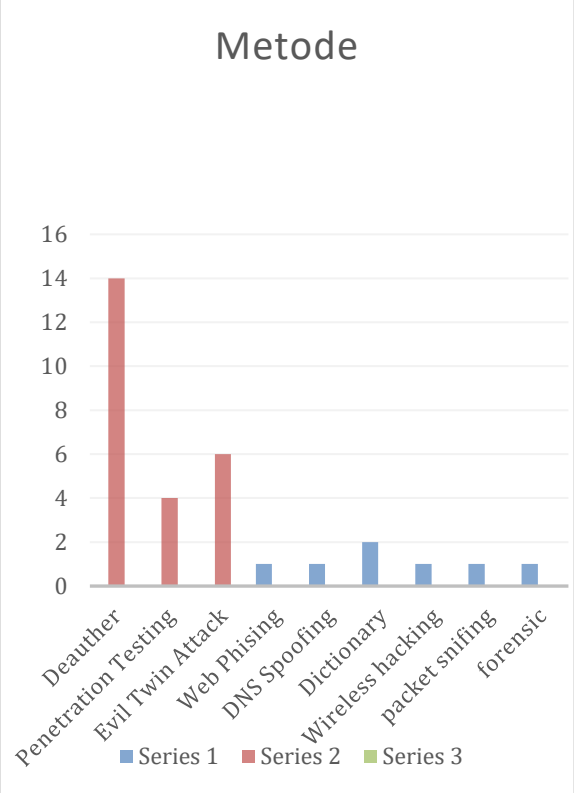
15.	W. Iman	Sistem…[15]	2020	*Deauther* dan *Rogue Access Point*	Serangan	*Wifi-Pumkin*
16.	A. Azmi, J. Gusti	Analisis…[16]	2022	*Deauther Attack*	Keamanan	*Aireplay-ng*
17.	I. Achmad Rizal Fauzi	Monitoring…[17]	2018	*Packet Sniffing*	Serangan	*Ettercap*
18.	M. Hanafi	Analisa…[18]	2023	*Penetration Testing*	Keamanan	*Forensic*
19.	D.Ruswati, D. Susilo	Uji…[19]	2023	*Deauther Attack*	Keamanan	*AeroWPA*
20.	H. Wintolo, I. Riadi	Analisis…[20]	2025	*Network Forensic Development Life Cycle*	Keamanan	*Tripwire*
21.	Y.Mulyanto, dkk	Analisis…[21]	2022	*Peneration Testing*	Keamanan	*Aircrack-ng*
22.	A. Saraun, dkk	An Analysis…[22]	2021	*Peneration Testing*	Keamanan	*Airodump-ng*
23.	N. Sitohang	Analisis…[23]	2020	*Dictionary Attack*	Keamanan	*Aircrack-ng*

Beberapa poin penting dari tabel tersebut antara lain:

a. Distribusi Tahun Publikasi
   Mayoritas artikel berasal dari tahun 2020 ke atas, menunjukkan bahwa topik ini masih sangat relevan dan aktif diteliti hingga saat ini.
b. Metode Serangan yang Diidentifikasi
   Metode yang paling sering digunakan adalah Deauthentication Attack, baik sebagai metode utama maupun dikombinasikan dengan serangan lain seperti Evil Twin dan Man-in-the-Middle. Metode lain yang juga muncul adalah DNS Spoofing, Dictionary Attack, dan Packet Sniffing.
c. Jenis Pengujian
   Sekitar 70% artikel berfokus pada pengujian keamanan, yang bertujuan untuk mencegah serangan, sedangkan sisanya melakukan simulasi serangan langsung untuk menguji kerentanan sistem. Jenis pengujian mencakup evaluasi firewall, sistem autentikasi, serta sistem monitoring lalu lintas jaringan.
d. Tools yang Digunakan
   Tools yang paling sering muncul adalah: Aircrack-ng: untuk brute-force dan packet sniffing. Fluxion: untuk simulasi Evil Twin Attack dan phishing login. ESP8266: digunakan dalam simulasi serangan berbasis perangkat IoT. Tools pendukung lainnya termasuk: Ettercap, Aireplay-ng, Airodump-ng, Airbase-ng, Arcai.com, dan WiFi Pumpkin.
e. Tren Penelitian
   Ada kecenderungan untuk menggabungkan beberapa tools dan metode dalam satu penelitian guna memperluas cakupan simulasi dan pengujian. Beberapa penelitian juga sudah mulai menggunakan WPA3 dan IDS untuk menguji efektivitas pertahanan terhadap serangan.

4.2. Metode untuk menganalisis *Wireless Access Point*

Pembahasan dari pertanyaan yang telah dibuat ditentukan dari research Question. Metode yang dilakukan peneliti terdahulu yang dijadikan referensi terkait topik serangan deauthentication attack pada wireless access Point.



Grafik 1. Grafik jumlah metode untuk menganalisis Wireless Access Point

Berdasarkan grafik yang telah disajikan, terdapat empat metode yang telah diusulkan oleh para peneliti sebelumnya dalam menganalisis serangan terhadap Wireless Access Point. Metode-metode tersebut meliputi Deauther, Penetration Testing, Evil Twin Attack, Web Phishing, Wireless Hacking, Packet Sniffing, Forensic, dan Dictionary. Dari hasil tinjauan berbagai makalah penelitian yang telah dilakukan, ditemukan bahwa terdapat dua metode utama yang paling sering digunakan dalam penelitian keamanan jaringan nirkabel, yaitu Deauthentication dan Evil Twin Attack.

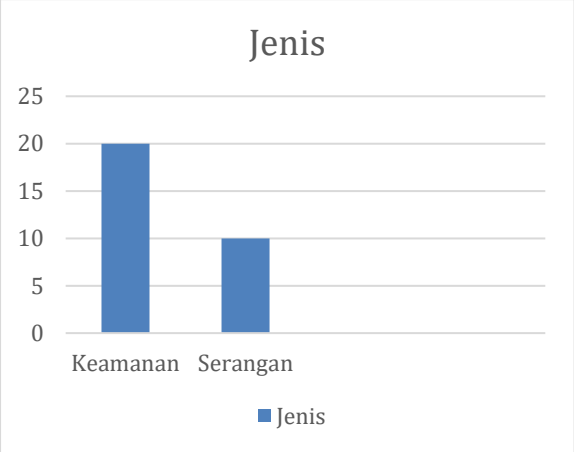
Dapat dilihat dengan jelas bahwa metode deauthentication merupakan teknik yang paling umum digunakan untuk menyerang jaringan Wireless Access Point dibandingkan dengan metode lainnya. Hal ini menunjukkan bahwa metode ini memiliki potensi ancaman yang lebih signifikan terhadap keamanan

jaringan Wi-Fi, terutama dalam skenario di mana pengguna tidak memiliki kesadaran tinggi terhadap ancaman siber.

Metode deauthentication attack bekerja dengan cara memuturs koneksi antara perangkat klien dan Wireless Access Point (WAP) dengan mengirimkan paket deauthentication frames secara terus-menerus. Serangan ini termasuk dalam katagori Denial of Service (DoS) karena mengganggu koneksi tanpa harus mengetahui kata sandi Wi-Fi.

Popularitas serangan ini meningkat karena kemudahannya dalam eksekusi, efektivitas dalam mengganggu koneksi, serta sering digunakan dalam serangan lanjutan seperti Evil Twin Attack dan Man-in-the-Middle (MITM) Attack. Berbagai alat seperti Aircrack-ng, MDK4, dan ESP8266 Deauther semakin mempercepat adopsi serangan ini di kalangan peretas maupun penguji penetrasi jaringan.

4.3. Jenis-Jenis unutk menganalisis *Wireless Access Point*



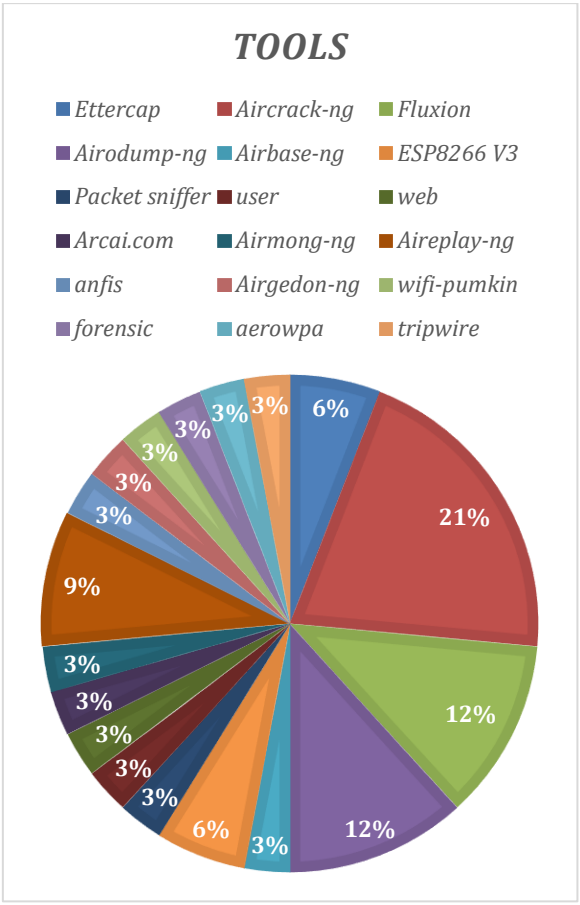
Grafik 2. Grafik jumlah jenis untuk menganalisis Wireless Access Point

Dari grafik diatas pengujian pada Wireless Access Point (WAP) lebih sering berfokus pada keamanan karena jaringan nirkabel rentan terhadap berbagai ancaman siber. Tujuan utama dari pengujian ini adalah memastikan bahwa WAP dikonfigurasi dengan baik dan memiliki perlindungan yang cukup untuk mencegah akses ilegal dan serangan dari luar. Salah satu hal yang diuji adalah penggunaan sistem enkripsi yang kuat, seperti WPA2 atau WPA3, yang berfungsi untuk melindungi data agar tidak mudah disadap. Selain itu, metode autentikasi juga diperiksa untuk memastikan bahwa hanya pengguna yang sah yang bisa masuk ke jaringan. Pengujian keamanan juga mencakup pemeriksaan firewall, sistem deteksi ancaman, dan pencatatan aktivitas jaringan untuk mendeteksi potensi serangan.

Selain aspek keamanan, pengujian juga dilakukan terhadap berbagai jenis serangan untuk menemukan celah yang bisa dimanfaatkan oleh peretas. Beberapa contoh serangan yang diuji adalah Man-in-the-Middle (MitM), di mana peretas mencoba menyadap dan mengubah data yang dikirimkan antara pengguna dan jaringan, serta serangan deautentikasi, yang bertujuan untuk memutus koneksi pengguna dari jaringan. Pengujian ini juga bisa mencakup upaya peretasan kata sandi dengan Teknik Evil Twin Attack.

Meskipun pengujian serangan penting untuk mengetahui seberapa kuat perlindungan WAP terhadap ancaman, pengujian keamanan tetap lebih sering dilakukan. Hal ini karena pengujian keamanan bersifat pencegahan, memastikan bahwa sistem sudah memiliki perlindungan yang cukup sebelum terjadi serangan. Sementara itu, pengujian serangan lebih berfokus pada menemukan kelemahan yang bisa dimanfaatkan oleh peretas setelah sistem berjalan. Oleh karena itu, dalam menjaga keamanan jaringan, pengujian terhadap perlindungan dan pencegahan ancaman menjadi prioritas utama agar jaringan tetap aman, stabil, dan dapat diandalkan.

4.4. Alat-alat untuk menganalisis *Wireless Access Point*



Grafik 3. Grafik jumlah tools untuk menganalisis Wireless Access Point

Berdasarkan diagram diatas untuk menguji keamanan jaringan Wireless Access Point (WAP), ada banyak tools yang bisa digunakan, masing-masing dengan fungsi dan keunggulannya sendiri. Salah satu yang paling sering digunakan adalah Aircrack-ng. Tool ini dirancang khusus untuk menguji seberapa kuat keamanan jaringan Wi-Fi dengan cara

menganalisis data yang ditransmisikan, menguji enkripsi, dan mencoba membobol kata sandi menggunakan teknik brute force. Karena kemampuannya yang andal dalam menguji keamanan jaringan, Aircrack-ng menjadi pilihan utama dalam pengujian WAP.

Selain Aircrack-ng, ada juga Fluxion, yang bisa menjadi alternatif karena memiliki hampir semua fitur dari berbagai tools lainnya. Fluxion bekerja dengan Teknik Evil Twin Attack, yaitu membuat jaringan palsu yang terlihat seperti jaringan asli untuk mendapatkan informasi login pengguna secara diam-diam. Karena sifatnya yang lebih fleksibel dan mencakup berbagai metode serangan, Fluxion sering digunakan untuk pengujian keamanan yang lebih mendalam.

Selain dua tools utama tersebut, ada juga tools lain yang sering digunakan untuk berbagai tujuan dalam pengujian keamanan jaringan. Airodump-ng digunakan untuk menangkap dan menganalisis lalu lintas data dalam jaringan, sementara Aireplay-ng berguna untuk menguji respon keamanan jaringan dengan mengirimkan paket data tertentu. Airbase-ng berfungsi untuk membuat jaringan palsu dalam simulasi serangan terhadap WAP.

Tools lain yang sering dipakai termasuk Ettercap, yang digunakan dalam serangan Man-in-the-Middle (MitM) untuk menyadap atau mengubah komunikasi dalam jaringan, serta ESP8266 V3, yang sering dipakai dalam simulasi serangan berbasis perangkat IoT. Packet Sniffer dan User Web Arcai.com membantu dalam memonitor lalu lintas jaringan serta mendeteksi aktivitas mencurigakan yang bisa menjadi tanda adanya serangan. Airgedon-ng dan WiFi-Pumpkin digunakan dalam serangan berbasis phishing, yang bertujuan untuk mendapatkan informasi login pengguna dengan cara menipu mereka agar memasukkan kredensial mereka ke dalam jaringan palsu.

Selain itu, ada Forensic Aerowpa, yang lebih berfokus pada analisis forensik jaringan untuk melacak aktivitas mencurigakan dan memastikan keamanan data. Tripwire adalah tool yang digunakan untuk mendeteksi perubahan yang mencurigakan pada file penting dalam jaringan, membantu administrator dalam mengidentifikasi potensi ancaman sejak dini. Airmon-ng memungkinkan perangkat Wi-Fi masuk ke mode pemantauan sehingga pengguna bisa menangkap dan menganalisis lalu lintas data lebih mendalam.

Deauthentication Attack adalah metode serangan paling dominan karena kemudahannya dalam pelaksanaan dan efektivitas dalam memutus koneksi pengguna. Tools Aircrack-ng dan Fluxion terbukti sebagai alat paling banyak digunakan karena fleksibilitas dan kekuatannya dalam pengujian keamanan. Pengujian yang dilakukan lebih banyak bersifat pencegahan dengan fokus pada perlindungan dan pemantauan akses terhadap jaringan. Berdasarkan hasil literatur yang ditinjau, langkah-langkah seperti penerapan enkripsi WPA3, penggunaan Intrusion Detection System (IDS), serta edukasi pengguna sangat penting dalam mencegah serangan Deauthentication. Dengan demikian, hasil penelitian menegaskan bahwa pendekatan pengujian yang bersifat preventif dan penggunaan tools yang tepat merupakan kunci utama dalam menjaga keamanan Wireless Access Point. Temuan ini memberikan dasar yang kuat bagi pengembangan sistem perlindungan jaringan Wi-Fi yang lebih tangguh di masa mendatang.

5. KESIMPULAN DAN SARAN

Dari hasil penelitian, dapat disimpulkan bahwa serangan *Deauthentication Attack* merupakan metode yang paling sering digunakan terhadap *Wireless Access Point* (*WAP*). Serangan ini dapat menyebabkan gangguan koneksi yang signifikan tanpa memerlukan pengetahuan tentang kata sandi jaringan. Beberapa tools yang umum digunakan dalam pengujian keamanan jaringan *Wi-Fi* adalah *Aircrack-ng* dan *Fluxion*. Penggunaan *WPA3*, *Intrusion Detection Systems* (*IDS*), serta kesadaran pengguna tentang potensi ancaman menjadi langkah pencegahan yang penting untuk menjaga keamanan jaringan.

Penelitian selanjutnya disarankan untuk fokus pada pengembangan teknik mitigasi yang lebih efektif terhadap serangan *Deauthentication* dan metode serangan lainnya yang terkait dengan *Wi-Fi*. Penelitian dapat juga mengkaji pengujian keamanan yang melibatkan kombinasi berbagai teknik serangan untuk mendapatkan gambaran lebih komprehensif mengenai celah keamanan yang ada dalam *Wireless Access Point*. Penggunaan metode baru untuk mendeteksi dan mencegah serangan ini akan sangat berguna untuk memperkuat perlindungan jaringan *Wi-Fi* di masa depan.

Secara keseluruhan, meskipun serangan *Deauthentication* merupakan ancaman yang cukup sering digunakan, masih banyak potensi untuk mengembangkan strategi mitigasi yang lebih kuat. Langkah-langkah pencegahan seperti penerapan *WPA3*, penggunaan *IDS*, serta pemahaman lebih dalam oleh pengguna tentang ancaman *Wi-Fi* sangat penting. Penelitian di masa mendatang diharapkan dapat mengembangkan metode baru yang lebih canggih untuk menghadapi perkembangan teknik serangan yang terus berubah.

DAFTAR PUSTAKA

[1] T. Pangestu and R. Liza, "Analisis Keamanan Jaringan Pada Jaringan Wireless Dari Serangan Man In The Middle Attack DNS Spoofing," *JiTEKH*, vol. 10, no. 2, pp. 60–67, 2022, doi: 10.35447/jitekh.v10i2.571.

[2] Satria Galang Saputra, B. Parga Zen, and Abdurahman, "Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing Execution Standard (PTES)," *J. Sist. Inf. Galuh*, vol. 1, no. 2, pp. 43–51, 2023, doi: 10.25157/jsig.v1i2.3152.

[3] L. Muhammad, Z. Fikri, A. Zafrullah, and A.

Zubaidi, "Analisis Keamanan Jaringan Wi-Fi Dengan Metode Deauthentication Attack Pada Access point Di Lingkungan Universitas Mataram (Wi-Fi Network Security Analysis With Deauthentication Attack Method At Access point In The University Of Mataram)".

[4] S. E. Prasetyo and T. Windranata, "Perbandingan Sistem Autentikasi Wpa2 Eap-Psk Pada Jaringan Wireless Dengan Metode Penetration Testing Menggunakan Fluxion Tools," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 7, no. 1, pp. 43–51, 2022, doi: 10.36341/rabit.v7i1.2206.

[5] M. N. Fauzan, A. M. dan Z. Arifin, and Mahfud, "WIRELESS ATTACK : MENGGUNAKAN TOOLS AIRCRACK PADA KALI LINUX UNTUK MELAKUKAN WPA ATTACK," *J. Lentera*, vol. 20, no. 1, pp. 1–73, 2021.

[6] "Kali Linux Documentation," *Wirel. Secur. Test. Tool. Retrieved*, 2022, [Online]. Available: https://www.kali.org

[7] D. Erisma Faishol, T. Adi Cahyanto, and M. Rahman, "Analisis Dan Evaluasi Protokol Keamanan Jaringan Nirkabel Wi-Fi Protected Access 3 dengan Metode Penetration Testing," *J. Ris. Sist. Inf. Dan Tek. Inform. (JURASIK*, vol. 9, no. 1, pp. 420–432, 2024, [Online]. Available: https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

[8] M. E. Rahmat and T. Desyani, "Implementasi Pengamanan Jaringan Dengan Teknik Penetration TestingMenggunakan Metode DeautherDan Evil Twin Pada WirelessTl-WR840N," *OKTAL OKTAL J. Ilmu Komput. dan Sci.*, vol. 3, no. 4, pp. 885–899, 2024, [Online]. Available: https://journal.mediapublikasi.id/index.php/oktal

[9] A. Aman, "Pengujian Keamanan Jaringan Nirkabel Melalui Simulasi Serangan Man In The Middle Attack Di Sekolah XYZ," *Digit. Transform. Technol.*, vol. 3, no. 2, pp. 824–831, 2023, doi: 10.47709/digitech.v3i2.3378.

[10] A. Andika Putra, "Analisis Dan Evaluasi Keamanan Wireless Lan Pada Pt. Bumi Jage Dalam," *Pros. Semin. Nas. Ilmu Komput.*, vol. 1, no. 1, p. 2021, 2021.

[11] I. M. Lina and G. R. Fernandes, "Analisis Pola Sosial Engineering Menggunakan Teknik Wifi Deauther Dan Evil Twin," *JRKT (Jurnal Rekayasa Komputasi Ter.*, vol. 2, no. 04, pp. 253–260, 2022, doi: 10.30998/jrkt.v2i04.8185.

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

[13] T. Ariyadi, I. Irham, and E. F. Cahyadi, "An Evaluation of Wireless Network Security with Penetration Testing Method at PT PLN UP2D S2JB," *J. Infotel*, vol. 16, no. 1, pp. 1–8, 2024, doi: 10.20895/infotel.v16i1.1057.

[14] I. Ramadhan, H. B. Seta, and R. Astriratma, "Pengamanan Wireless Local Area Network Dari Serangan Arp Spoofing Menggunakan Pendekatan Deteksi Pasif Dan Deauthentication Attack Berbasis Rasp," *Senamika*, pp. 761–770, 2020, [Online]. Available: https://conference.upnvj.ac.id/index.php/senamika/article/view/617

[15] W. Iman, "Sistem Deteksi Serangan Rogue Access Point," 2020. [Online]. Available: https://en.wikipedia.org/wiki/Rogue_access_point

[16] A. Y. F. Azmi, J. Gusti A G, and E. Wahyudi, "Analisis Network Security pada Layanan Wifi Indihome Terhadap Serangan Denial of Service (DOS)," *J. Litek J. List. Telekomun. Elektron.*, vol. 19, no. 1, pp. 8–12, 2022, doi: 10.30811/litek.v19i1.18.

[17] I. M. S. Achmad Rizal Fauzi, "MONITORING JARINGAN WIRELESS TERHADAP SERANGAN PACKET SNIFFING DENGAN MENGGUNAKAN IDS Achmad".

[18] M. A. Hanafi, "ANALISA KEAMANAN JARINGAN WIRELESS UNIMMA MENGGUNAKAN METODE PENETRATION TESTING," Universitas Muhammadiyah Magelang, 2023.

[19] D. Ruswanti, D. Susilo, F. Sains, and U. S. Surakarta, "Uji keamanan wpa2 dengan wi-fi deauther menggunakan aerowpa 1,2," vol. 6, pp. 860–866, 2023, doi: 10.37600/tekinkom.v6i2.776.

[20] H. Wintolo, I. Riadi, and A. Yudhana, "Analisis Deteksi Penyusup pada Layanan Open Journal System Menggunakan Metode Network Forensic Development Life Cycle," vol. 8, pp. 133–144, 2025.

[21] Y. Mulyanto, H. Herfandi, and R. Candra Kirana, "ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING (Studi kasus:RS H.LMANAMBAI ABDULKADIR)," *J. Inform. Teknol. dan Sains*, vol. 4, no. 1, pp. 26–35, 2022, doi: 10.51401/jinteks.v4i1.1528.

[22] A. Saraun, A. S. M. Lumenta, and D. Febrian Sengkey, "An Analysis of WLAN Security at the Minahasa Regency Office of Educational Affairs," *J. Tek. Inform.*, vol. 17, no. 1, pp. 565–572, 2021.

[23] N. Sitohang, "Analisis Kelemahan Keamanan pada Jaringan Wireless," *Anal. Keamanan Jar. Wirel.*, vol. XI, no. 1, pp. 38–46, 2020.