

# Evaluasi *Penetration Testing* Terhadap Kerentanan Jaringan WLAN Yang Menggunakan WPA2

Nizam, Leonardus Sandy Ade Putra, Fitri Imansyah

Jurusan Teknik Elektro

Fakultas Teknik

Universitas Tanjungpura Pontianak

email : [nizambest3@gmail.com](mailto:nizambest3@gmail.com)

## Abstrak

Perkembangan teknologi nirkabel menghadirkan kemudahan akses informasi, namun juga menimbulkan tantangan serius terkait keamanan jaringan. Penelitian ini bertujuan untuk menganalisis tingkat kerentanan *Wireless Local Area Network* (WLAN) dengan menggunakan metode *Penetration Testing*. Pengujian difokuskan pada protokol keamanan WPA 2 yang umum digunakan dengan skenario serangan berupa *Cracking The Encryption* dan *Man in the Middle Attack (MITM)*. Metode penelitian dilakukan melalui serangkaian tahapan mulai dari *network monitoring*, *Packet Capture*, *deauthentication attack*, hingga upaya *encryption key cracking* menggunakan *Aircrack-ng*. Selain itu, simulasi serangan MITM dilaksanakan dengan memanfaatkan *Ettercap* melalui teknik ARP poisoning untuk mengintersepsi komunikasi jaringan. Hasil penelitian menunjukkan bahwa upaya *cracking* terhadap SSID target tidak berhasil dikarenakan keterbatasan *wordlist*, sedangkan simulasi serangan MITM berhasil memperoleh data sensitif pada jaringan terbuka. Berdasarkan hasil tersebut, dapat disimpulkan bahwa meskipun jaringan WLAN dengan WPA2 memiliki tingkat keamanan lebih baik dibandingkan metode enkripsi sebelumnya, potensi kerentanan masih dapat dimanfaatkan apabila konfigurasi dan kontrol keamanan tidak diperkuat. Oleh karena itu, diperlukan implementasi strategi keamanan tambahan seperti penggunaan kata sandi yang kuat, pembaruan konfigurasi perangkat, serta peningkatan pengawasan jaringan untuk meminimalisasi risiko ancaman siber.

**Kata kunci:** *Cracking The Encryption, Keamanan Jaringan, Penetration Testing*

## Abstract

*Advances in wireless technology have made it easier to access information, but they have also raised serious challenges regarding network security. This study aims to analyze the vulnerability of Wireless Local Area Networks (WLANs) using Penetration Testing methods. The testing focused on the widely used WPA2 security protocol, with attack scenarios including "Cracking The Encryption" and "Man-in-the-Middle" (MITM) attacks. The research methodology involved a series of steps ranging from network monitoring, Packet Capture, and deauthentication attacks to attempts to crack encryption keys using Aircrack-ng. Additionally, a MITM attack simulation was conducted using Ettercap via ARP poisoning techniques to intercept network communications. The results showed that attempts to crack the target SSID were unsuccessful due to limitations in the wordlist, whereas the MITM attack simulation successfully obtained sensitive data on an open network. Based on these results, it can be*

*concluded that although WLAN networks with WPA2 offer a higher level of security compared to previous encryption methods, potential vulnerabilities can still be exploited if security configurations and controls are not strengthened. Therefore, the implementation of additional security strategies—such as the use of strong passwords, device configuration updates, and enhanced network monitoring—is necessary to minimize the risk of cyber threats.*

**Keywords:** *Cracking the Encryption, Network Security, Penetration Testing*

## I. LATAR BELAKANG

Perkembangan teknologi semakin lama semakin maju dengan pesat mendorong manusia untuk menciptakan teknologi baru yang dapat lebih bermanfaat dan mempermudah pekerjaan manusia. Tentunya perkembangan teknologi tersebut akan membuat laju informasi di dunia ini semakin cepat. Laju informasi yang begitu cepatnya membuat manusia harus mampu mengolah berbagai informasi yang ada untuk memperoleh suatu hasil data yang diinginkan[1]. Perkembangan teknologi komunikasi ini juga didukung dengan semakin meningkatnya kemajuan infrastruktur dan teknologi komunikasi dan informasi ini adalah komunikasi menggunakan *wireless*. Ini ditandai dengan perkembangan munculnya peralatan nirkabel yang telah menggunakan standar protokol *Wireless Fidelity (WiFi)* yang berbasis standar IEEE 802.11[2]. Penggunaan jaringan yang semakin luas di dunia bisnis dan pertumbuhan kebutuhan penggunaan internet online services yang semakin cepat mendorong untuk memperoleh keuntungan dari *shared data* dan *shared resources*[3].

Pengguna di seluruh dunia memanfaatkan *WiFi* untuk beragam tujuan, mencakup sektor pendidikan, bisnis, dan perdagangan, bahkan adopsinya telah meluas hingga ke kalangan anak-anak. Namun penggunaan *WiFi* tidak lepas dari berbagai risiko keamanan seperti *phishing*, *sniffing*, *hacking*, *cracking*, dan bentuk kejahatan siber lainnya[4]. Universitas Tanjungpura Pontianak sebagai salah satu institusi pendidikan tinggi terkemuka, menyediakan berbagai fasilitas penunjang kegiatan akademik dan non-akademik, termasuk akses internet nirkabel. Fasilitas ini krusial tidak hanya bagi mahasiswa dan dosen untuk mendukung kegiatan pembelajaran dan penelitian, tetapi juga bagi berbagai unit di lingkungan Universitas untuk operasional sehari-hari. Sebagai contoh, di Laboratorium Telekomunikasi Fakultas Teknik Universitas Tanjungpura Pontianak, akses internet nirkabel dimanfaatkan secara ekstensif untuk simulasi jaringan, pengujian perangkat, dan akses ke sumber daya komputasi awan yang menunjang riset di bidang telekomunikasi.

Namun, di balik kemudahan akses yang ditawarkan oleh jaringan nirkabel, terdapat potensi risiko keamanan siber yang signifikan. Peningkatan ancaman kejahatan siber, seperti pencurian data melalui *sniffing*, penyebaran malware, atau serangan *phishing*, menjadi perhatian serius. Meskipun pengelolaan jaringan seringkali dilakukan oleh staf atau administrator teknis, pengawasan tersebut seringkali terbatas pada jam kerja operasional[5]. Serangan siber, di sisi lain, dapat terjadi kapan saja, termasuk di luar jam pengawasan langsung, sehingga meningkatkan kerentanan sistem[6].

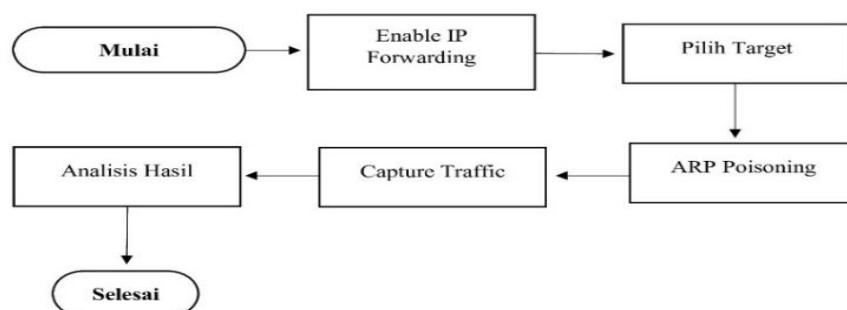
Oleh karena itu, sangat penting bagi Laboratorium Telekomunikasi Fakultas Teknik Universitas Tanjungpura Pontianak, untuk memastikan bahwa infrastruktur jaringan dan data yang dikelola terlindungi dari berbagai ancaman. Dalam upaya mitigasi risiko tersebut, penelitian ini akan melakukan pengujian keamanan data menggunakan metode *Penetration Testing*[7]. Pengujian ini bertujuan untuk menganalisis dan mengevaluasi efektivitas sistem keamanan teknologi WLAN khususnya pada lapisan autentikasi dan enkripsi nirkabel yang telah diterapkan di lingkungan Laboratorium Telekomunikasi Fakultas Teknik Universitas Tanjungpura Pontianak, guna mengidentifikasi potensi kerentanan dan merekomendasikan perbaikan yang diperlukan.

## II. METODE PENELITIAN

Penelitian ini akan mendalami dua metode serangan siber yang umum digunakan untuk mengeksploitasi kerentanan dalam sistem keamanan digital: *Cracking In Encryption* dan *Man in the Middle* (MITM) Attack. Kedua pendekatan ini menyoroti bagaimana penyerangan dapat mengkompromikan kerahasiaan dan integritas data, serta implikasinya terhadap privasi dan keamanan informasi[8]. *Cracking In Encryption* mengacu pada proses pemecahan atau penguraian enkripsi untuk mengungkapkan data asli yang tersembunyi. Tujuan utamanya adalah untuk mendapatkan akses tidak sah ke informasi rahasia yang seharusnya dilindungi oleh enkripsi[9]. *Man in the Middle* (MITM) Attack adalah jenis serangan di mana penyerang secara diam-diam mencegat dan mungkin mengubah komunikasi antara dua pihak yang percaya bahwa mereka sedang berkomunikasi secara langsung satu sama lain. Serangan ini seringkali memanfaatkan kerentanan dalam protokol jaringan atau konfigurasi yang tidak aman untuk menempatkan diri mereka di jalur komunikasi[10].

### 1. *Cracking The Encryption*

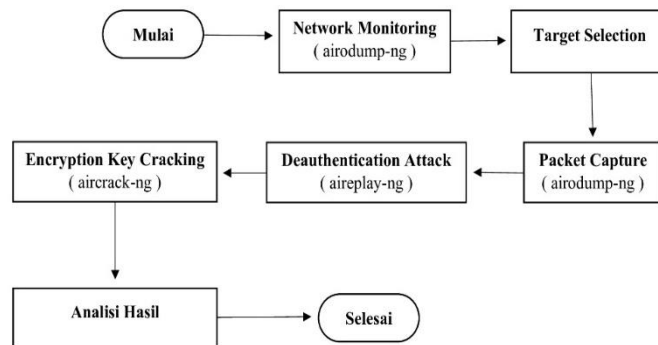
Tujuan dari studi ini adalah untuk mengevaluasi sejauh mana *Access Point* terlindungi oleh skema enkripsi seperti WEP, WPA, dan WPA2. Analisis ini akan menggunakan pendekatan *Brute-force Attack*, yang secara sistematis menguji setiap kombinasi kunci enkripsi yang mungkin hingga akses berhasil didapatkan. Durasi proses ini sangat dipengaruhi oleh panjang kunci dan kerumitan algoritma yang digunakan. Detail alur kerja *Cracking The Encryption* selanjutnya dapat dilihat pada gambar 1.



Gambar 1. Alur Kerja *Cracking The Encryption*

### 2. *Man in the Middle Attack* (MITM)

Pengujian ini menggunakan aplikasi *Ettercap* sebagai alat uji. Analisa menggunakan metode *ARP spoofing*, dimana penyerangan mencoba mengubah tabel *Address Resolution Protocol* (ARP) di jaringan lokal. Tujuannya adalah untuk mengisi tabel ARP *host* jaringan dengan alamat MAC yang salah yang dikendalikan oleh penyerangan. Ini memungkinkan pencuri untuk mengontrol lalu lintas jaringan melalui mesin mereka, memungkinkan mereka untuk melacak, menyadap, atau memanipulasi komunikasi antara dua entitas. Berikut flowchart *Man in the Middle* Attack yang dapat dilihat pada gambar dibawah ini.



Gambar 2. Alur Kerja *Man in the Middle* Attack

### III. HASIL DAN PEMBAHASAN

Pada penelitian ini, dilakukan serangkaian keamanan jaringan Wireless Local Area Network (WLAN) dengan menggunakan metode *Penetration Testing*. Pengujian dilakukan dengan mensimulasikan dua jenis serangan utama, yaitu *Cracking The Encryption* dan *Man in the Middle* (MITM) Attack, guna mengidentifikasi tingkat kerentanan jaringan terhadap ancaman eksternal. Seluruh pengujian terhadap aplikasi web pada penelitian ini dilakukan secara etis dan terbatas pada lingkungan yang memang disediakan untuk tujuan edukasi dan pengujian keamanan. Situs *testphp.vulnweb.com* merupakan aplikasi web demonstrasi publik yang secara resmi disediakan oleh perusahaan keamanan aplikasi Acunetix sebagai target latihan dan pengujian kerentanan yang legal. Selain itu, pengujian pada *techpanda.org* dilakukan hanya untuk mengamati implementasi protokol HTTPS dan mekanisme enkripsi TLS tanpa melakukan eksploitasi terhadap sistem. Dengan demikian, seluruh aktivitas pengujian dalam penelitian ini tidak ditujukan pada sistem produksi tanpa izin, melainkan pada lingkungan yang diperuntukkan untuk pembelajaran, simulasi, dan evaluasi keamanan secara terkendali.

#### **Proses Pengujian *Cracking The Encryption* Terhadap Access Point ftuntan Menggunakan *Aircrack-ng***

Analisa menggunakan metode *Brute force Attack*, di mana serangan mencoba semua kemungkinan kombinasi kunci enkripsi untuk mendapatkan akses. Dibutuhkan *Dictionary Word*, *Handshake* user lain, Channel yang digunakan dan BSSID dari *Access Point*. Berikut

merupakan langkah-langkah yang dilakukan oleh peneliti dalam proses *Cracking The Encryption*.

### Network Monitoring

Perintah *airodump-ng wlan0* dijalankan untuk melakukan pemindaian terhadap jaringan WiFi di sekitar, menggunakan adaptor WiFi yang telah diaktifkan dalam mode monitor.

```
(nizu@kali)-[~]
$ sudo su
(root@kali)-[/home/nizu]
# airodump-ng wlan0
```

Gambar 3. Command Network Monitoring

Berikut ini adalah hasil *Network Monitoring* yang dapat dilihat pada gambar dibawah ini.

| BSSID             | PWR | Beacons | #Data, #/s | CH | MB | ENC CIPHER | AUTH      | ESSID               |
|-------------------|-----|---------|------------|----|----|------------|-----------|---------------------|
| 16:18:D6:04:DF:F5 | -86 | 3       | 0          | 0  | 1  | 195        | WPA2 CCMP | PSK <length: 0>     |
| D2:21:F9:1E:DC:13 | -58 | 9       | 0          | 0  | 6  | 130        | WPA2 CCMP | PSK <length: 0>     |
| D2:21:F9:1E:DE:7D | -78 | 10      | 0          | 0  | 11 | 130        | WPA2 CCMP | PSK <length: 0>     |
| 78:8A:20:51:9E:77 | -93 | 6       | 0          | 0  | 1  | 130        | OPN       | Untan               |
| 7E:8A:20:57:37:4D | -34 | 13      | 0          | 0  | 6  | 130        | WPA2 CCMP | PSK <length: 0>     |
| 82:8A:20:57:37:4D | -34 | 13      | 0          | 0  | 6  | 130        | WPA2 CCMP | PSK <length: 0>     |
| 82:8A:20:51:95:B8 | -38 | 17      | 0          | 0  | 11 | 130        | WPA2 CCMP | PSK <length: 0>     |
| 7E:8A:20:51:95:B8 | -33 | 17      | 0          | 0  | 11 | 130        | WPA2 CCMP | PSK <length: 0>     |
| 78:8A:20:57:37:4D | -34 | 57      | 31         | 0  | 6  | 130        | OPN       | Untan               |
| 8C:83:E8:82:CE:CC | -82 | 12      | 0          | 0  | 6  | 130        | WPA2 CCMP | PSK PRODI.ARS 2.4 G |
| D0:21:F9:6E:E0:75 | -1  | 0       | 0          | 0  | 7  | -1         |           | <length: 0>         |
| D0:21:F9:6E:DC:13 | 0   | 51      | 739        | 10 | 6  | 130        | WPA2 CCMP | PSK ftuntan         |
| D2:21:F9:1E:D5:A1 | -64 | 12      | 0          | 0  | 1  | 130        | WPA2 CCMP | PSK <length: 0>     |
| D0:21:F9:6E:D5:A1 | -68 | 28      | 122        | 8  | 1  | 130        | WPA2 CCMP | PSK ftuntan         |
| 04:18:D6:04:DF:F5 | -90 | 9       | 109        | 16 | 1  | 195        | OPN       | Untan               |
| 78:8A:20:51:95:B8 | -32 | 80      | 97         | 0  | 11 | 130        | OPN       | Untan               |
| 78:8A:20:51:99:06 | -1  | 0       | 13         | 0  | 11 | -1         | OPN       | <length: 0>         |
| D0:21:F9:6E:DE:7D | -83 | 28      | 3          | 0  | 11 | 130        | WPA2 CCMP | PSK ftuntan         |

Gambar 4. Hasil Nework Monitoring

### Target Selection

Berdasarkan hasil *Network Monitoring* yang disajikan, terlihat daftar BSSID (*Basic Service Set Identifier*) beserta informasi terkait seperti kekuatan sinyal (PWR), jumlah *beacon*, data frame, kanal (Ch), dan jenis enkripsi (ENC CIPHER). Dengan menetapkan “ftuntan” sebagai target, langkah-langkah selanjutnya dalam metodologi akan difokuskan secara eksklusif pada BSSID yang terkait dengan ESSID ini, yaitu D0:21:F9:6E:DC:13, untuk melakukan akuisisi data yang lebih terarah dan analisis kerentanan yang mendalam. Fokus pada target tunggal ini memungkinkan alokasi sumber daya komputasi yang efisien dan meminimalkan interferensi dengan jaringan lain yang tidak relevan dengan cakupan penelitian.

### Packet Capture

Berdasarkan data hasil *Network Monitoring* awal, telah berasosiasi dengan ESSID “ftuntan” dan beroperasi pada kanal 6. Informasi ini, yang diperoleh dari fase “*Network Monitoring*”, menjadi basis empiris untuk konfigurasi utilitas penangkapan paket. Perintah berikut ini diaplikasikan untuk melakukan akuisisi (*Packet Capture*) terhadap *Basic Service Set Identifier* (BSSID) yang berasosiasi dengan *Extended Service Set Identifier* (ESSID) “ftuntan”.

```
(root@kali)-[/home/nizu]
# airodump-ng --bssid D0:21:F9:6E:DC:13 -c 6 -w result1 wlan0
22:54:49 Created capture file "result1-01.cap".
```

Gambar 5. Command Packet Capture

Berikut adalah tampilan yang setelah melakukan perintah *Packet Capture*, dapat dilihat pada gambar di bawah ini.

| BSSID             | PWR               | RXQ | Beacons | #Data, #/s | CH   | MB     | ENC   | CIPHER | AUTH | ESSID   |
|-------------------|-------------------|-----|---------|------------|------|--------|-------|--------|------|---------|
| D0:21:F9:6E:DC:13 | -60               | 87  | 439     | 5077       | 8    | 6 130  | WPA2  | CCMP   | PSK  | ftuntan |
| BSSID             | STATION           |     | PWR     | Rate       | Lost | Frames | Notes | Probes |      |         |
| D0:21:F9:6E:DC:13 | DE:03:6F:8C:8E:C2 |     | -71     | 24e-24e    | 0    | 685    |       |        |      |         |
| D0:21:F9:6E:DC:13 | 34:E1:2D:0F:B2:4D |     | -77     | 1e- 6e     | 0    | 100    |       |        |      |         |
| D0:21:F9:6E:DC:13 | 5E:3E:2F:FE:57:A0 |     | -90     | 24e- 1e    | 4    | 4571   |       |        |      |         |
| D0:21:F9:6E:DC:13 | 62:AC:9F:FE:F0:C9 |     | -70     | 24e- 1e    | 7    | 210    |       |        |      |         |

Gambar 6. Hasil Packet Capture

### Deauthentication Attack

Berdasarkan data yang telah teridentifikasi dari fase *Packet Capture*, *target Access Point* (AP) adalah ESSID “ftuntan” dengan BSSID D0:21:F9:6E:DC:13, dan telah diidentifikasi pula sebuah klien yang terhubung dengan alamat MAC DE:03:6F:8C:8E:C2. Berikut perintah dan hasil dari *Deauthentication Attack* dapat dilihat pada gambar dibawah ini.

```
(root@kali)-[/home/nizu]
# aireplay-ng --deauth 10 -a D0:21:F9:6E:DC:13 -c DE:03:6F:8C:8E:C2 wlan0
11:12:56 Sending 64 directed DeAuth (code 7). STMAC: [AC:74:B1:45:80:21] [10]41 ACKs]
11:12:56 Sending 64 directed DeAuth (code 7). STMAC: [AC:74:B1:45:80:21] [90]94 ACKs]
11:12:57 Sending 64 directed DeAuth (code 7). STMAC: [AC:74:B1:45:80:21] [ 7]40 ACKs]
11:12:58 Sending 64 directed DeAuth (code 7). STMAC: [AC:74:B1:45:80:21] [18]52 ACKs]
11:12:58 Sending 64 directed DeAuth (code 7). STMAC: [AC:74:B1:45:80:21] [105]107 ACKs]
11:12:59 Sending 64 directed DeAuth (code 7). STMAC: [AC:74:B1:45:80:21] [ 8]40 ACKs]
11:12:59 Sending 64 directed DeAuth (code 7). STMAC: [AC:74:B1:45:80:21] [48]82 ACKs]
```

Gambar 7. Command Deauthentication Attack

Tujuan utama dari serangan ini adalah untuk memprovokasi klien target agar melakukan re-authentication dengan AP, sehingga menghasilkan *four-way Handshake* WPA/WPA2 yang dapat ditangkap oleh *airodump-ng* yang beroperasi secara simultan. Keberhasilan serangan ini akan secara langsung mempengaruhi keberhasilan fase “*Packet Capture*” dalam memperoleh *Handshake* WPA/WPA2 yang valid. Tanpa *Handshake* ini, tahapan selanjutnya yaitu “*Encryption Key Cracking*” tidak akan dapat dilanjutkan. Oleh karena itu, *Deauthentication Attack* berfungsi sebagai katalisator untuk akuisisi informasi kritis yang diperlukan untuk analisis keamanan lebih lanjut.

### Encryption Key Cracking

Berdasarkan data yang telah berhasil diakumulasi dari fase *Packet Capture* dan *Deauthentication Attack*, yaitu *four-way WPA/WPA2 Handshake* yang terekam dalam file *Packet Capture* “/home/nizu/result1-01.cap” yang berasosiasi dengan BSSID D0:21:F9:6E:DC:13, *Aircrack-ng* digunakan untuk mengimplementasikan offline dictionary

```
(root@kali)-[/home/nizu]
# aircrack-ng -w Desktop/untan.txt -b D0:21:F9:6E:DC:13 /home/nizu/result1-01.cap
```

attack. Berikut perintah yang digunakan untuk melakukan *Encryption Key Cracking*, dapat dilihat pada gambar dibawah ini.

Gambar 8. *Command Encryption Key Cracking*

Keberhasilan tahap ini secara langsung berbanding lurus dengan kualitas dan cakupan *wordlist* yang digunakan, serta entropi dari passphrase target . Passphrase yang memiliki entropi rendah atau merupakan bagian dari daftar kata sandi umum akan lebih rentan terhadap serangan ini.

### **Hasil dan Analisa Pengujian *Cracking The Encryption Terhadap Access Point ftuntan Menggunakan Aircrack-ng.***

Berdasarkan pengujian *Cracking The Encryption* menggunakan metode *Penetration Testing* didapatkan hasil yang dapat dilihat pada gambar dibawah ini.



```
Aircrack-ng 1.7
[00:03:25] 2424479/2424479 keys tested (11998.89 k/s)
Time Left: --
KEY NOT FOUND

Master Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
               00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
               00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
               00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
               00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Gambar 9. Hasil *Encryption Key Cracking*

Tangkapan layar yang disajikan merupakan output terminal dari eksekusi utilitas aircrack versi 1.7, yang secara definitif mengindikasikan kegagalan proses pemulihan *Pre-Shared Key* (PSK) dari jaringan nirkabel target. Hasil ini merupakan validasi empiris dari efektivitas offline dictionary attack yang telah diimplementasikan, karena kata sandi yang benar tidak ditemukan dalam *wordlist* yang digunakan. Proses pembuatan *wordlist* ini dilakukan dengan memanfaatkan *Large Language Model* (LLM) Chat CPT untuk melakukan generate kombinasi kata sandi secara otomatis. Parameter yang dimasukkan ke dalam sistem AI tersebut meliputi entitas lokasi dan jaringan (seperti "ftuntan", "teknik", dan "elektro"), profil personel dosen yang berafiliasi dengan laboratorium, serta instruksi untuk menghasilkan variasi minimal 8 karakter dengan penggabungan huruf kapital, angka, dan tanda khusus seperti @ (*at symbol*), \_(*underscore*), ! (*exclamation mark*), dan # (*hashtag*).

Setelah seluruh kombinasi kata sandi tersebut disusun ke dalam satu direktori data, tahap selanjutnya adalah melakukan pengujian menggunakan alat *Aircrack-ng*. Namun, berdasarkan skenario serangan yang telah diupayakan secara maksimal tersebut, hasil eksekusi *Aircrack-ng* secara definitif menyatakan kegagalan serangan dengan keluaran "KEY NOT FOUND". *Wordlist* berhasil menguji sejumlah 2.424.479 hipotesis kata sandi hingga batas *wordlist* tercapat, yang mengindikasikan bahwa proses komputasi untuk offline dictionary attack telah berjalan dengan efisien dan tuntas.

Untuk memvalidasi kondisi teknis serangan, peneliti merujuk pada analisis paket jaringan yang dihasilkan oleh *Wireshark*. Analisis tersebut secara tegas mengonfirmasi bahwa data krusial, yaitu *four-way Handshake* WPA/WPA2, telah berhasil diakuisisi secara in toto.

Adanya  
rangkaian  
EAPOL  
lengkap  
Message 1

| No. | Time     | Source           | Destination       | Protocol | Length | Info                 |
|-----|----------|------------------|-------------------|----------|--------|----------------------|
| ... | 86.40... | Ubiquiti1_6e:... | 6a:35:a8:30:15... | EAPOL    | 1...   | Key (Message 1 of 4) |
| ... | 86.48... | 6a:35:a8:30:...  | Ubiquiti_6e:dc... | EAPOL    | 2...   | Key (Message 2 of 4) |
| ... | 86.51... | Ubiquiti_6e:...  | 6a:35:a8:30:15... | EAPOL    | 3...   | Key (Message 3 of 4) |
| ... | 86.51... | 6a:35:a8:30:...  | Ubiquiti_6e:dc... | EAPOL    | 1...   | Key (Message 4 of 4) |

paket  
yang  
dari  
hingga

Message 4, secara empiris membuktikan terpenuhinya prasyarat kriptografis yang esensial untuk rekoveri *Pre-Shared Key* (PSK).

Gambar 10. *Four-Way Handshake* WPA/WPA2

Dengan demikian, ketika *Handshake* yang utuh (dibuktikan oleh *Wireshark*) gagal dipecahkan oleh *Aircrack-ng*, kesimpulannya adalah kata sandi yang benar tidak ada di dalam *wordlist* yang diuji. Kegagalan ini bukan karena cacat pada data yang ditangkap atau program *Aircrack-ng*, melainkan karena *wordlist* yang digunakan tidak cukup komprehensif untuk mencakup kata sandi yang dibuat oleh pemilik jaringan, yang kemungkinan besar unik, panjang, atau menggunakan kombinasi karakter yang tidak umum.

### Proses Pengujian *Man in the Middle Attack* Terhadap Tingkat Keamanan Website

Pengujian ini menggunakan aplikasi *Ettercap* sebagai alat uji. Pendekatan ini memungkinkan mengamati cara kerja dan dampak serangan *Man In The Middle Attack* dalam kerangka yang terkontrol dan etis, tanpa mengorbankan integritas data atau melanggar regulasi yang berlaku. Berikut adalah tahapan-tahapan metodologis yang dilaksanakan dalam simulasi *Man in the Middle Attack*

#### Enable IP Forwarding

Langkah untuk mengaktifkan IP Forwarding dengan menuliskan perintah “*sudo sysctl -w net.ipv4.ip\_forward=1*” pada terminal linux berikut adalah tampilan dari mengaktifkan IP Forwarding dapat dilihat pada gambar dibawah ini.

```
nizu@kali ~$ sudo sysctl -w net.ipv4.ip_forward=1
[sudo] password for nizu:
net.ipv4.ip_forward = 1
```

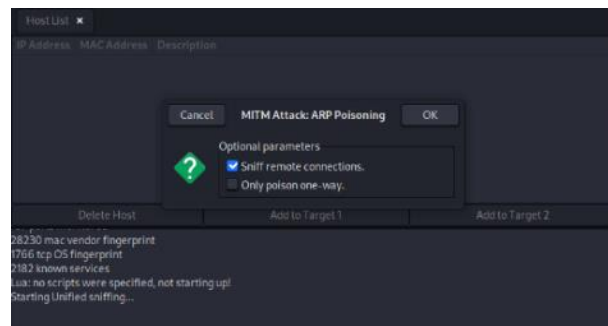
Gambar 11. *Command Enable IP Forwarding*

#### Pilih Target

Fase ini berfokus pada identifikasi dan determinasi entitas komunikasi yang akan menjadi objek serangan *Address Resolution Protocol (ARP) Poisoning*. Target 1 secara tipikal diidentifikasi sebagai Gerbang Jaringan (*Gateway*), mengingat perannya sebagai titik agregasi seluruh lalu lintas *inbound* dan *outbound* dalam segmen jaringan lokal. Manipulasi *ARP cache* pada gateway ini memfasilitasi pengalihan lalu lintas yang semestinya ditujukan kepada host korban. Sementara itu, target 2 merepresentasikan Perangkat Korban (*host*), yakni endpoint komunikasi yang lalu lintasnya menjadi objek pemantauan atau manipulasi melalui manipulasi *ARP cache* pada perangkat korban, lalu lintas akan diarahkan secara paksa menuju gateway atau entitas jaringan lainnya melalui infrastruktur penyerang.

### **ARP Poisoning**

Tahap ini merupakan inti dari serangan *Man in the Middle Attack* yang memanfaatkan manipulasi *Address Resolution Protocol (ARP)*, di mana tool *Etercap* akan digunakan untuk menyuntikkan informasi ARP palsu ke dalam jaringan. Tampilan menu *ARP Poisoning* dapat dilihat pada gambar dibawah ini.



Gambar 12. Proses *ARP Poisoning*

### **Analisa Pengujian *Man in the Middle Attack* Terhadap Website Kategori HTTP**

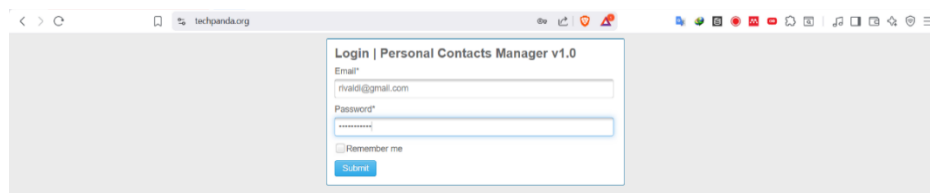
Mengingat keterbatasan akses data lapangan dan potensi implikasi legalitas yang mungkin timbul dari penelitian tanpa izin, studi ini akan memanfaatkan situs web <http://testphp.vulnweb.com> sebagai lingkungan simulasi untuk investigasi serangan *Man in the Middle Attack*. Setelah berhasil diimplementasikannya fase *ARP Poisoning* yang mengakibatkan pengalihan lalu lintas data melalui node penyerang. Tampilan interface menunjukkan konfirmasi keberhasilan injeksi *ARP spoofing*. Kemudian, log yang terekam secara *real-time* memperlihatkan aliran data HTTP dari situs web simulasi <http://testphp.vulnweb.com>, termasuk di dalamnya adalah informasi sensitif berupa kredensial pengguna (*username=test&password=test*) yang berhasil diintersepsi. Data yang tertangkap ini menjadi bukti empiris keberhasilan serangan *Man in the Middle Attack* dalam mengakses komunikasi yang seharusnya bersifat pribadi.

Keberhasilan intersepsi kredensial pada situs simulasi tersebut berakar pada karakteristik dasar protokol *Hypertext Transfer Protocol (HTTP)* yang tidak memiliki lapisan keamanan *Transport Layer Security (TLS)*. Skenario serangan ini *Etercap* berperan sebagai jembatan yang melakukan manipulasi pada tabel ARP milik korban dan gateway. Dengan teknik *ARP Poisoning*, *Etercap* memaksa lalu lintas data yang seharusnya menuju server untuk dialihkan

terlebih dahulu ke perangkat penyerang. Karena data tidak terenkripsi, *Etercap* secara otomatis dapat melakukan pemindaian (*sniffing*) dan mengekstraksi string teks sensitif secara *real-time*. Fenomena ini membuktikan bahwa meskipun enkripsi pada lapisan nirkabel (WPA2) sudah aktif, data tetap rentan selama protokol komunikasi di lapisan aplikasi tidak menyediakan enkripsi *end-to-end*.

### Analisa Pengujian *Man in the Middle Attack* Terhadap Website Kategori HTTPS

Analisis mendalam menunjukkan bahwa kegagalan dalam proses *sniffing* ini diakibatkan oleh protokol yang digunakan oleh web server yaitu HTTPS.



Gambar 13. Tampilan Login Techpanda.org

Komputer target mengakses situs <https://techpanda.org/> dan memasukkan user [rivaldi@gmail.com](mailto:rivaldi@gmail.com) serta passwordnya “smansadj\*\*a”. Namun pada saat komputer tester berusaha untuk merekam, pada saat komputer target membuka situs <https://techpanda.org/> aplikasi *Etercap* mengalami kegagalan. Setelah dianalisis ditemukan kegagalan dalam proses sniffing berasal dari protokol yang digunakan oleh web server, yaitu HTTPS. HTTPS beroperasi melalui mekanisme enkripsi *Transport Layer Security* (TLS), yang secara teoretis memproteksi integritas dan kerahasiaan informasi dari pihak ketiga. Lebih lanjut, ketika laptop target kemudian mencoba mengakses situs techpanda dengan mengetikkan secara manual <http://techpanda.org/> pada kolom URL peramban Google Chrome, URL tersebut secara otomatis kembali menjadi HTTPS.

Oleh karena itu, dapat disimpulkan bahwa faktor kegagalan dalam intersepsi lalu lintas pada kasus ini bukan disebabkan oleh konfigurasi keamanan yang dimiliki oleh jaringan WLAN di Laboratorium Telekomunikasi, melainkan lebih dominan pada konfigurasi keamanan web server dari situs yang diakses, khususnya adopsi HTTPS. Hal ini menunjukkan keterbatasan serangan *Man in the Middle Attack* berbasis *ARP Poisoning* ketika berhadapan dengan koneksi yang terenkripsi dan terlindungi oleh mekanisme keamanan protokol tingkat tinggi.

### Hasil Pengujian *Penetration Testing*

Berdasarkan serangkaian simulasi yang telah dilakukan, efektivitas keamanan jaringan *Wireless Local Area Network* (WLAN) dievaluasi melalui dua skenario serangan utama. Rekapitulasi hasil dari keseluruhan implementasi pengujian tersebut disajikan secara komprehensif pada tabel di bawah ini.

Tabel 1. Hasil *Penetration Testing*

| No | Jenis Serangan | Variabel Kunci / Informasi | Status Serangan | Keterangan Singkat |
|----|----------------|----------------------------|-----------------|--------------------|
|----|----------------|----------------------------|-----------------|--------------------|

|   |                                 |                                             |          |                                                                             |
|---|---------------------------------|---------------------------------------------|----------|-----------------------------------------------------------------------------|
| 1 | <i>Cracking The Encryption</i>  | <i>Handshake , Wordlist, BSSID, Channel</i> | GAGAL    | Kata sandi tidak terdaftar dalam dictionary <i>wordlist</i> yang diujikan.  |
| 2 | <i>Man-In-The-Middle (MITM)</i> | WLAN Access, Target IP Address              | BERHASIL | Berhasil mengintersepsi lalu lintas data pada protokol non-enkripsi (HTTP). |

Berdasarkan hasil pengujian pada tabel tersebut, skenario *Cracking The Encryption* menunjukkan status gagal. Hal ini terjadi meskipun seluruh parameter teknis, seperti paket handshake yang utuh dan identitas *Access Point* (BSSID serta Channel), telah terpenuhi secara valid. Kegagalan ini membuktikan bahwa metode *brute-force* atau dictionary attack memiliki ketergantungan mutlak pada kualitas data referensi (*wordlist*). Dalam kasus ini, kata sandi yang digunakan oleh target memiliki tingkat kompleksitas yang tinggi dan kemungkinan berupa kombinasi karakter alfanumerik panjang yang tidak terdapat dalam daftar kata standar. Secara akademis, hasil ini menegaskan bahwa enkripsi WPA2 masih memberikan proteksi yang sangat kuat terhadap serangan *offline* selama pengguna menerapkan kebijakan kata sandi yang kuat.

Berbeda dengan pengujian pertama, skenario *Man in the Middle Attack* mencapai status berhasil. Keberhasilan ini dimungkinkan karena penyerangan telah berhasil memperoleh akses ke dalam jaringan WLAN yang sama dengan target, yang memperoleh akses ke dalam jaringan WLAN yang sama dengan target, yang merupakan syarat utama dalam melakukan ARP *spoofing*. Dengan memposisikan perangkat penyerangan di antara klien dan gateway, lalu lintas data dapat diintersepsi secara *real-time*. Hasil pengujian menunjukkan bahwa protokol yang tidak terenkripsi seperti HTTP, sangat rentan terhadap teknik ini, di mana informasi sensitif dapat diekstraksi keamanan pada lapisan aplikasi yang tetap dapat dieksploitasi meskipun lapisan keamanan nirkabel (WPA2) sulit ditembus melalui metode *cracking*.

#### IV. KESIMPULAN

Berdasarkan hasil pengujian keamanan jaringan *Wireless Local Area Network* (WLAN) menggunakan metode *Penetration Testing* pada jaringan ftuntan, dapat disimpulkan bahwa protokol keamanan WPA2 masih memiliki tingkat ketahanan yang baik terhadap serangan *Cracking The Encryption*, yang dibuktikan dengan kegagalan proses *offline dictionary attack* menggunakan *Aircrack-ng* yang menghasilkan keluaran berupa status "KEY NOT FOUND". Hasil tersebut menunjukkan bahwa meskipun peneliti berhasil memperoleh four-way Handshake WPA/WPA2 yang lengkap dan valid, kata sandi yang digunakan oleh target tidak ditemukan di dalam *wordlist* yang diuji. Validitas data Handshake telah dikonfirmasi melalui analisis menggunakan Wireshark yang memperlihatkan keberadaan paket EAPOL secara lengkap dari Message 1 hingga Message 4, sehingga dapat dipastikan bahwa kegagalan proses *cracking* bukan disebabkan oleh kesalahan pada proses packet capture, kerusakan file hasil tangkapan, maupun kesalahan pada alat pengujian, melainkan karena kata sandi yang digunakan memiliki tingkat kompleksitas yang tinggi dan tidak termasuk dalam kumpulan kata sandi pada *wordlist* yang digunakan.

Temuan ini menunjukkan bahwa implementasi WPA2 dengan penggunaan kata sandi yang kuat, panjang, dan sulit diprediksi masih mampu memberikan perlindungan yang efektif terhadap serangan *brute-force* maupun *offline dictionary attack*. Di sisi lain, hasil pengujian *Man-in-the-Middle* (MITM) menunjukkan bahwa keamanan pada lapisan enkripsi nirkabel tidak sepenuhnya menjamin keamanan komunikasi data secara menyeluruh, karena serangan berbasis ARP *Poisoning* masih dapat mengintersepsi lalu lintas data pada protokol yang tidak menerapkan enkripsi *end-to-end*, seperti HTTP, sedangkan pengujian terhadap situs yang menggunakan protokol HTTPS menunjukkan bahwa mekanisme *Transport Layer Security* (TLS) mampu menjaga kerahasiaan data dan mencegah proses penyadapan informasi sensitif. Oleh karena itu, keamanan jaringan WLAN tidak hanya bergantung pada penggunaan protokol WPA2, tetapi juga memerlukan penerapan kata sandi yang kuat, penggunaan protokol komunikasi yang aman seperti HTTPS, pembaruan konfigurasi perangkat secara berkala, serta peningkatan kesadaran pengguna terhadap praktik keamanan siber guna meminimalkan risiko ancaman terhadap kerahasiaan, integritas, dan ketersediaan data.

## V. REFERENSI

- [1] M. I. Rusdi and D. Prasti, "Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux," 2019.
- [2] B. Adhi Prakosa, "Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method," 2020. [Online]. Available: <https://iocscience.org/ejournal/index.php/mantik>
- [3] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.
- [4] A. A. Najar and S. Manohar Naik, "Cyber-Secure SDN: A CNN-Based Approach for Efficient Detection and Mitigation of DDoS attacks," *Comput. Secur.*, vol. 139, p. 103716, Apr. 2024, doi: 10.1016/J.COSE.2024.103716.
- [5] Y. Yanti and J. T. Imum Lueng Bata Batoh -Banda ceh, "Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WiFi," *Serambi Engineering*, vol. III, no. 1, 2018.
- [6] S. U. Sunaringtyas, D. Surya Prayoga, J. K. Siber, P. Siber, and S. Negara, "Edu Komputika Journal Implementasi Penetration Testing Execution Standard Untuk Uji Penetrasi Pada Layanan Single Sign-On," 2021. [Online]. Available: <http://journal.unnes.ac.id/sju/index.php/edukom>
- [7] U. Bina, D. Palembang, H. D. Sabdho, and M. Ulfa, "Seminar Hasil Penelitian Vokasi (Semhavok) Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor Pt. Mora Telematika Indonesia Regional Palembang".
- [8] N. A. Santoso, M. Ainurohman, and R. D. Kurniawan, "PENERAPAN METODE PENETRATION TESTING PADA KEAMANAN JARINGAN NIRKABEL," *JURNAL RESPONSIF*, vol. 4, no. 2, pp. 162–167, 2022, [Online]. Available: <https://ejurnal.ars.ac.id/index.php/jti>
- [9] M. Hasibuan and A. M. Elhanafi, "Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan

- Metode Black Box,” *sudo Jurnal Teknik Informatika*, vol. 1, no. 4, pp. 171–177, Dec. 2022, doi: 10.56211/sudo.v1i4.160.
- [10] E. Ginting, P. Sahara, and S. Nurhaliza Tambunan, “UNES Journal of Information System Ancaman Denial Of Service Attack Dalam Eksploitasi Keamanan Sistem Informasi Threat Of Denial Of Service Attack In Information System Security Exploitation,” 2023, [Online]. Available: <https://fe.ekasakti.org/index.php/UJIS>