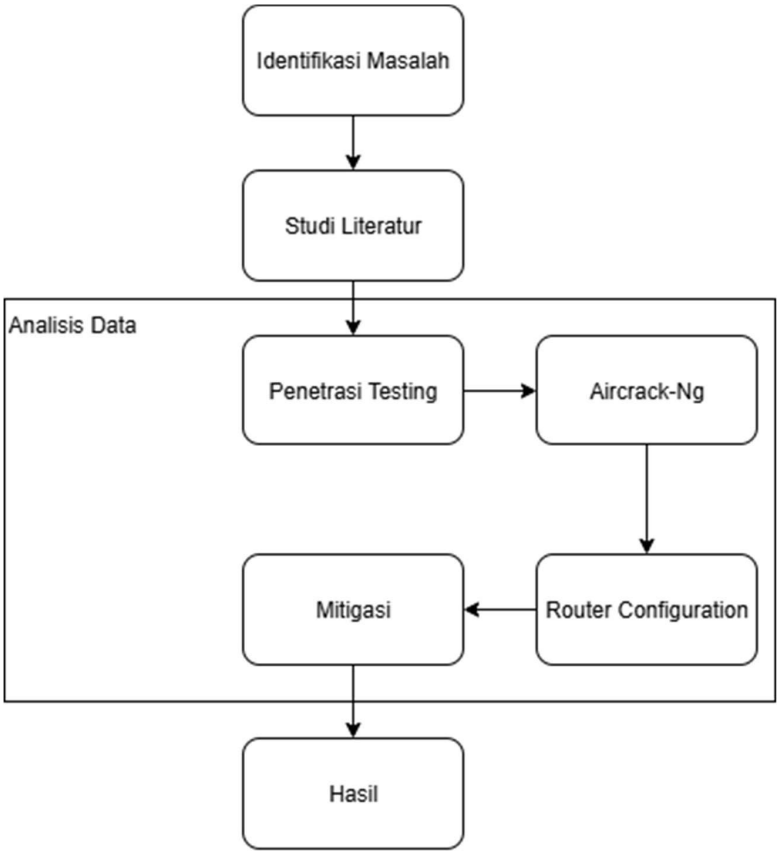
# BAB III

# METODE PENELITIAN

## 3.1 Desain Penelitian

Berikut ini merupakan desain penelitian tentang implementasi tools *aircrack-ng* untuk menganalisis keamanan jaringan wifi, dimulai dari tahap identfikasi masalah, studi literatur, penetrasi *testing* menggunakan *aircrack-ng*, mitigasi, dan penentuan hasil. Adapun detail desain penelitian sebagai berikut:




**Gambar 3. 1** Desain Penelitian

(**Sumber :** Data Penelitian 2025)

Penelitian ini diawali dengan identifikasi masalah yang menjadi fokus utama dalam kajian keamanan jaringan WiFi. Setelah permasalahan berhasil dirumuskan, penulis melanjutkan ke tahap studi literatur untuk mengkaji teori-teori serta penelitian sebelumnya yang relevan sebagai dasar dalam menyusun kerangka penelitian. Studi literatur ini juga berfungsi sebagai panduan dalam merancang metode yang akan diterapkan pada tahap berikutnya.

Tahap inti dari penelitian berada dalam proses analisis data, yang dimulai dengan penetrasi testing menggunakan tools seperti *Aircrack-ng* untuk menguji tingkat keamanan jaringan WiFi. *Aircrack-ng* berperan dalam melakukan serangan terhadap jaringan guna mengidentifikasi potensi celah, khususnya pada aspek autentikasi. Hasil dari proses ini kemudian dianalisis lebih lanjut melalui *router configuration*, yaitu peninjauan dan evaluasi terhadap konfigurasi perangkat *router*, seperti pengaturan *WPS, SSID, dan password*, yang seringkali menjadi titik lemah.

Berdasarkan temuan dari tahapan tersebut, penulis merancang strategi mitigasi yang difokuskan pada perbaikan konfigurasi dan penguatan sistem keamanan jaringan. Langkah mitigasi ini bertujuan untuk menutup celah keamanan yang ditemukan serta meningkatkan daya tahan jaringan terhadap serangan.

Akhir dari seluruh proses ini menghasilkan hasil penelitian yang mencakup evaluasi efektivitas metode yang diterapkan, kesimpulan atas temuan yang diperoleh, serta rekomendasi untuk peningkatan keamanan jaringan.

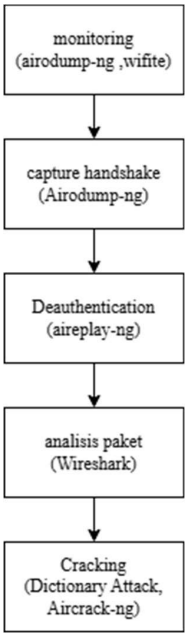
## 3.2 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah metode penetration testing. Metode ini merupakan pendekatan yang bersifat praktis

dan langsung, dengan cara mensimulasikan serangan terhadap jaringan nirkabel untuk mengidentifikasi celah atau kerentanan keamanan yang ada. Pengujian dilakukan dalam lingkungan *PT Evergrown Technology* dengan menggunakan perangkat dan *tools* yang umum digunakan dalam pengujian keamanan jaringan, seperti *Wireshark, Aircrack-ng*, atau sejenisnya.

### 3.3 Penetrasi *Testing*

Pada tahap ini, pengujian dilakukan untuk mengevaluasi kapasitas jaringan atau sistem untuk menahan serangan eksternal. *test* penetrasi, dilakukan dengan mensimulasikan serangan yang mungkin terjadi, baik dengan alat otomatis maupun manual, untuk mengidentifikasi celah keamanan yang mungkin dimanfaatkan oleh pihak yang tidak bertanggung jawab. Adapun Langkah-langkah dalam melakukan penetrasi *testing* pada penelitian ini diantaranya.




**Gambar 3. 2** Penetrasi Testing

(**Sumber :** Data Penelitian 2025)

Adapun langkah- Langkah untuk penetrasi testing dijelaskan sebagai barikut:

***1. Monitoring***

Tahap ini bertujuan untuk memantau dan mengidentifikasi jaringan nirkabel yang tersedia di sekitar lokasi uji. Proses dilakukan menggunakan *tools* seperti *Wifite* dan *Airodump-ng*, yang mampu menangkap sinyal dari *Access Point* (AP) serta perangkat klien yang terhubung. Informasi yang dikumpulkan pada tahap ini mencakup nama *SSID, BSSID*, kekuatan sinyal, dan jenis enkripsi yang digunakan.

***2. Capture Handshake***

Setelah jaringan target teridentifikasi, langkah selanjutnya adalah menangkap paket *handshake* yang terjadi saat klien melakukan proses autentikasi ulang ke *Access Point*. Penangkapan *handshake* dilakukan dengan memanfaatkan *Airodump-ng,* dibantu dengan teknik deautentikasi untuk memaksa klien terputus dan melakukan koneksi ulang, sehingga proses *handshake* dapat direkam.

***3. Deauthentication***

Untuk mempercepat proses, dilakukan teknik deautentikasi untuk memaksa perangkat klien terputus sementara, sehingga proses *handshake* dapat ditangkap saat perangkat mencoba tersambung kembali.

Ketika perangkat klien mencoba untuk terhubung kembali ke jaringan Wi-*Fi* tersebut, proses *handshake* akan berlangsung, dan pada saat itulah paket *handshake* dapat ditangkap

Selanjutnya, dilakukan proses analisis terhadap data *handshake* yang telah berhasil ditangkap, dengan menggunakan aplikasi Wireshark. Melalui *Wireshark*, peneliti dapat memeriksa detail paket yang terekam, termasuk informasi terkait

proses autentikasi antara klien dan *Access Point*. Analisis ini bertujuan untuk memastikan bahwa paket *handshake* yang diperoleh valid dan lengkap

**4. Analisis Paket**

Paket handshake yang berhasil ditangkap kemudian dianalisis menggunakan *Wireshark*. Analisis ini mencakup pemeriksaan struktur paket dan validitas informasi yang terkandung di dalamnya, terutama dalam hal proses autentikasi antara klien dan Akses poin. Tujuan tahap ini adalah memastikan bahwa data *handshake* yang diperoleh lengkap dan dapat digunakan dalam proses selanjutnya, yakni *dekripsi*

**5. Cracking**

Setelah memastikan bahwa paket *handshake* berhasil ditangkap, tahap selanjutnya adalah melakukan proses dekripsi menggunakan *Aircrack-ng*. Proses ini bertujuan untuk menguji kekuatan sandi jaringan Wi-Fi dengan melakukan serangan *dictionary attack*, yaitu mencocokkan hasil *handshake* dengan daftar kata sandi (*wordlist*) yang telah ada di kali linux. Jika salah satu entri dalam *wordlist* sesuai dengan kunci autentikasi yang digunakan oleh jaringan, maka kata sandi WiFi akan berhasil dipecahkan.

**3.4 Mitigasi**

Setelah dilakukan identifikasi kerentanan melalui teknik seperti *monitoring, capture handshake, deauthentication,* dan *cracking*, maka langkah selanjutnya yaitu memberikan rekomendasi perbaikan serta implementasi solusi untuk memperkuat sistem jaringan nirkabel.

Langkah-langkah mitigasi terhadap *dictionary attack* yang diterapkan atau direkomendasikan dalam penelitian ini meliputi:

1. Penggunaan Kata Sandi yang Kuat dan Kompleks

   Mengganti kata sandi jaringan secara berkala dengan kombinasi huruf besar, huruf kecil, angka, dan karakter khusus yang tidak umum (contoh: W!f1#S3cur3_2025). Panjang kata sandi minimal 12 karakter untuk memperbesar ruang pencarian (*search space*) sehingga serangan menjadi tidak efisien

2. Implementasi *MAC Address Filtering*

   Menerapkan penyaringan berdasarkan *MAC address* untuk membatasi perangkat yang dapat terhubung ke jaringan, meskipun metode ini bukan solusi utama, namun dapat menambah lapisan keamanan.

3. Menonaktifkan *WPS*

   *WPS* memudahkan koneksi perangkat ke jaringan tanpa perlu mengetikkan kata sandi, namun celah pada metode *PIN WPS* sangat rentan terhadap *brute force attack*. Oleh karena itu, fitur ini sebaiknya dinonaktifkan melalui pengaturan router untuk mencegah penyerang mendapatkan akses dengan lebih mudah.

## 3.5 Lokasi Dan Jadwal Penelitian

### 3.5.1 Lokasi Penelitian

Penelitian dilakukan pada jaringan nitkabel di PT. *Evergrown Technology*, yang berlokasi di Panbil Industrial Estate, B2 Lot 5, Jalan Ahmad Yani, Muka Kuning, Kota Batam, Kepulauan Riau, Indonesia.


**Gambar 3. 3** Map PT *Evergrown Technology*

(**Sumber :** Google Maps, Data Penelitian 2025)

### 3.5.2 Jadwal penelitian

Jadwal penelitian dimulai sampai dengan akhir penelitian tertera pada table di bawah.

**Tabel 3. 1** Jadwal Penelitian

| No | Kegiatan | April | | | | Mei | | | | Juni | | | | Juli | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 1 | Studi Literatur | | | | | | | | | | | | | | | | |
| 2 | Pengurusan Izin Penelitian | | | | | | | | | | | | | | | | |
| 3 | Penyediaan Perangkat | | | | | | | | | | | | | | | | |
| 4 | Uji Penetrasi Jaringan | | | | | | | | | | | | | | | | |
| 5 | Konfigurasi Jaringan | | | | | | | | | | | | | | | | |
| 6 | Penulisan Hasil Penelitian | | | | | | | | | | | | | | | | |

(**Sumber:** Data Penelitian, 2025)