# BAB II

# TINJAUAN PUSTAKA

## 2.1 Teori Dasar

Bab ini mengulas teori-teori dasar yang menjadi landasan pendekatan dan solusi permasalahan, serta menyajikan tinjauan terhadap penelitian-penelitian sebelumnya yang relevan.

### 2.1.1 Jaringan Komputer

Menurut (Ekklesia Tangkowit Et Al., 2021) Jaringan komputer merupakan kumpulan dua atau lebih perangkat komputer yang saling terhubung untuk memungkinkan pertukaran data. Informasi dapat ditransmisikan melalui media kabel maupun nirkabel, sehingga memungkinkan para pengguna jaringan komputer untuk saling berbagi data, menggunakan printer secara bersama-sama, dan menjalankan aplikasi yang sama secara bersamaan.

**Gambar 2. 1** Jaringan Komputer

(**Sumber :**appkey, 2020)

Beberapa manfaat yang dapat diperoleh dari adanya jaringan komputer antara lain adalah sebagai berikut:

1. Berbagi Data

   Melalui jaringan komputer, pengguna dapat saling mengirim dan menerima file maupun dokumen dengan cepat tanpa perlu menggunakan media penyimpanan eksternal seperti *USB*. Hal ini mendukung kerja sama antar pengguna dan mempercepat proses kerja.

2. Berbagi Perangkat Keras

   Jaringan memungkinkan sejumlah komputer untuk memakai perangkat keras secara bersama, seperti *printer*, *scanner*, atau alat fotokopi. Dengan begitu, pengadaan perangkat menjadi lebih hemat karena tidak perlu menyediakan satu perangkat untuk setiap unit komputer.

3. Penggunaan Aplikasi Bersama

   Aplikasi yang diinstal pada *server* dapat diakses oleh beberapa pengguna secara bersamaan. Hal ini membantu dalam menghemat biaya lisensi dan memudahkan pengelolaan perangkat lunak.

4. Komunikasi Lebih Efisien

   Jaringan menyediakan sarana komunikasi seperti *email*, pesan instan, atau konferensi video, yang memudahkan interaksi antar pengguna baik dalam satu lokasi maupun dari tempat yang berjauhan.

5. Pusat Penyimpanan Data

   Melalui sistem jaringan, data disimpan di satu lokasi pusat (*server*), sehingga memudahkan proses pengelolaan, pencadangan, dan pengamanan informasi. Pengguna tetap dapat mengakses data tersebut dari perangkat masing-masing.

6. Penghematan Biaya

Karena berbagai sumber daya seperti data, perangkat keras, dan perangkat lunak dapat dimanfaatkan bersama, jaringan komputer dapat mengurangi biaya operasional dan meningkatkan efisiensi kerja.

### 2.1.2 Keamanan jaringan

Keamanan jaringan merupakan bidang ilmu dan praktik yang bertujuan untuk menjaga integritas, kerahasiaan, dan ketersediaan informasi serta sumber daya jaringan dari berbagai bentuk ancaman dan serangan. Di tengah pesatnya perkembangan era digital, pentingnya keamanan jaringan semakin meningkat karena banyaknya data dan sistem yang bergantung pada infrastruktur jaringan. Tanpa perlindungan yang memadai, jaringan dapat menjadi target serangan yang berdampak pada kerugian finansial, pencurian informasi, hingga penurunan reputasi. Oleh karena itu, pemahaman menyeluruh mengenai keamanan jaringan sangat diperlukan dengan mempelajari konsep, metode, serta teknologi utama yang digunakan dalam bidang ini.(Pratama & Yani No, 2023) Konsep dasar dalam keamanan jaringan mencakup beberapa elemen penting, di antaranya:

1. Kerahasiaan (*Confidentiality*)

   Kerahasiaan bertujuan untuk memastikan bahwa informasi yang ditransmisikan melalui jaringan hanya dapat diakses oleh pihak yang memiliki otorisasi. Salah satu metode utama yang digunakan untuk menjaga kerahasiaan adalah enkripsi. Enkripsi mengubah data menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang, dan hanya pihak yang memiliki kunci dekripsi yang sesuai dapat mengakses data aslinya. Contoh penerapan enkripsi dapat ditemukan pada protokol *SSL*/*TLS* (*Secure Sockets*

*Layer/Transport Layer Security*) yang digunakan untuk mengamankan komunikasi di internet.

2. Integritas (*Integrity*)

   Integritas menjamin bahwa data yang dikirimkan tidak mengalami perubahan atau kerusakan selama proses pengiriman. Untuk menjaga integritas data, digunakan teknik seperti *checksum* dan *hash*. Teknik ini memungkinkan penerima untuk memverifikasi bahwa data yang diterima sesuai dengan data yang dikirim. Salah satu protokol yang mendukung integritas adalah *IPsec* (*Internet Protocol Security*), yang menggunakan algoritma hash seperti *SHA* (*Secure Hash Algorithm*) untuk memastikan data tetap utuh selama transmisi.

3. Ketersediaan (*Availability*)

   Ketersediaan merupakan aspek penting lainnya dalam keamanan jaringan yang menjamin bahwa sumber daya jaringan dapat diakses oleh pengguna yang berwenang kapan pun dibutuhkan. Ancaman terhadap ketersediaan biasanya datang dari serangan *DoS (Denial of Service)* atau *DDoS (Distributed Denial of Service)*, di mana sistem dibanjiri oleh lalu lintas berlebih sehingga menyebabkan gangguan layanan. Untuk menangkal serangan semacam ini, digunakan berbagai solusi keamanan seperti *firewall*, sistem deteksi intrusi (*IDS*), dan sistem pencegahan intrusi (*IPS*).

4. Otentikasi (*Authentication*) dan Otorisasi (*Authorization*)

   Otentikasi berfungsi untuk memverifikasi bahwa pengguna atau perangkat yang berusaha mengakses jaringan benar-benar sah. Beberapa metode otentikasi yang umum digunakan termasuk penggunaan kata sandi, sertifikat

digital, serta otentikasi dua faktor (2FA). Setelah proses otentikasi berhasil, otorisasi berperan dalam menentukan hak akses pengguna. Otorisasi memastikan bahwa pengguna hanya bisa mengakses data atau layanan sesuai dengan izin yang diberikan berdasarkan peran atau kebijakan yang telah ditetapkan.

### 2.1.3 *Wireless Attack*

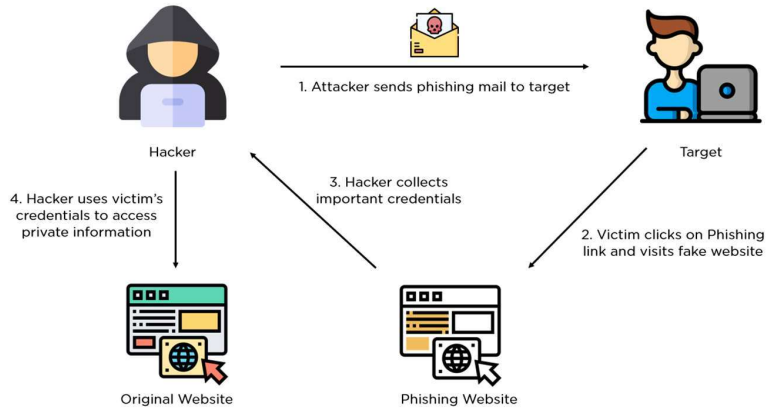
Serangan nirkabel, juga dikenal sebagai *Wireless Attack* merupakan jenis serangan siber yang menargetkan jaringan atau perangkat nirkabel (tanpa kabel), seperti *Wi-Fi*, *Bluetooth*, atau jaringan seluler. Serangan ini memanfaatkan kelemahan protokol komunikasi nirkabel untuk mendapatkan akses tidak sah, mencuri data, mengganggu koneksi, atau bahkan mengontrol perangkat korban. *Evil twin attack, packet sniffing, deauthentication attack*, dan *man-in-the-middle (MITM)* adalah beberapa contoh serangan nirkabel. Karena jaringan nirkabel dapat diakses secara fisik oleh siapa saja di sekitar jangkauan sinyal, serangan jenis ini sering kali lebih sulit dideteksi dan dicegah dibandingkan dengan serangan pada jaringan kabel. Oleh karena itu, menjaga jaringan nirkabel dengan enkripsi yang kuat dan autentikasi yang tepat sangat penting.(Susanto et al., 2019). bagian berikut akan membahas teknik-teknik serangan yang umum digunakan serta strategi mitigasi yang dapat diterapkan untuk mencegah atau meminimalkan dampaknya.

#### 2.1.3.1 Teknik Serangan

Adapun beberapa teknik serangan yang umum digunakan antara lain:

1. *Phishing*

Salah satu jenis serangan siber yang dikenal sebagai *phishing* adalah ketika pelaku berusaha menipu korban dengan memberikan informasi pribadi seperti nama pengguna dan kata sandi, informasi kartu kredit atau rekening *bank*, serta data pribadi seperti NIK, alamat, atau nomor telepon. Serangan ini biasanya dilakukan dengan berpura-pura menjadi orang yang dipercaya, seperti *bank, email*, media sosial, perusahaan besar, atau lembaga pemerintah. Pelaku sering mengirimkan pesan atau *email* palsu yang terlihat seperti pesan resmi dan berisi tautan ke situs palsu yang sangat mirip dengan situs asli. *Phishing* dapat termasuk *email* atau pesan mencurigakan yang memaksa korban untuk bertindak, *website* dengan *URL* yang tidak resmi, dan lampiran yang mengandung *malware*. (Putra et al., 2024)



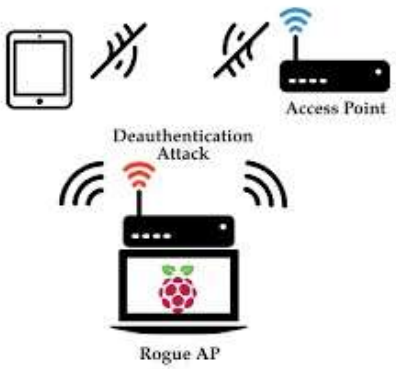

**Gambar 2. 2** Ilustrasi Serangan *Phising*

(**Sumber :** Rendy Islamy, 2022)

2. *Deauthentication Attack*

Tujuan dari serangan ini adalah untuk menangkap *handshake WPA/WPA2* dan kemudian di *crack* dengan mengirimkan sinyal palsu ke klien dan *access*

*point* agar mereka terputus dari jaringan *WiFi*. Dalam *Kali Linux*, penyerang menggunakan alat seperti *aireplay-ng*. (Jain et al., 2022) Serangan deautentikasi, juga dikenal sebagai salah satu jenis serangan pada jaringan nirkabel *(WiFi)* yang termasuk dalam kategori serangan *Denial of Service (DoS)*. Serangan ini menggunakan kelemahan protokol *IEEE 802.11*, terutama proses yang mengatur koneksi antara perangkat klien, seperti laptop atau *smartphone*, dan akses poin atau juga dikenal sebagai *router WiFi*. Protokol ini menggunakan *frame deauthentication* untuk memutuskan koneksi klien dari jaringan secara sah. Namun, frame ini tidak dienkripsi, sehingga penyerang dapat dengan mudah memalsukan frame dan mengirimkannya ke klien atau akses poin



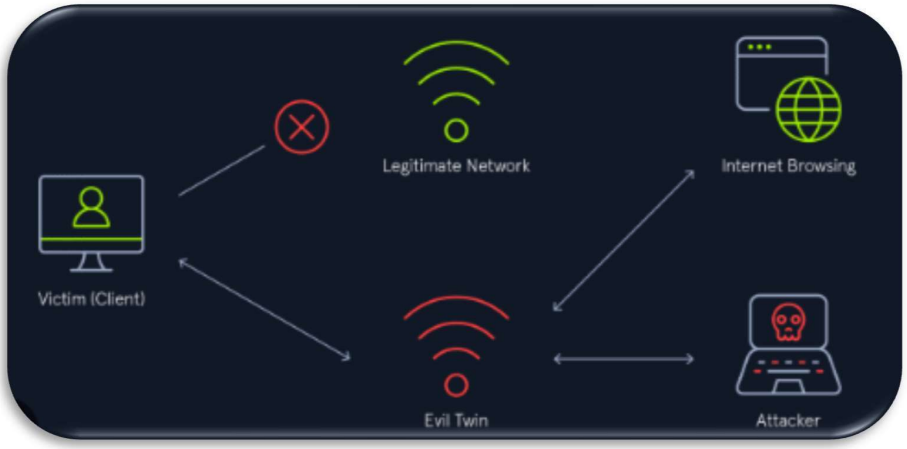

**Gambar 2. 3** Ilustrasi Serangan *Deauthentication*

(**Sumber :** Buckle, 2022).

3. *Evil Twin Attack*

   Serangan ini membuat *access point* palsu dengan *SSID* yang sama dengan Akses poin asli. Ketika korban terhubung tanpa sadar, data dapat disadap. Serangan ini dapat didukung oleh *Aircrack-ng dan Wireshark*. (Juhász et al.,

2019) Akses poin palsu biasanya memiliki nama *SSID (Service Set Identifier)* yang sama dengan akses poin asli. Setelah menghubungkan pengguna ke jaringan palsu, pencuri dapat melihat, mencegat, atau bahkan mengubah lalu lintas data pengguna, yang memungkinkan pencurian data pribadi seperti nama pengguna, kata sandi, atau informasi kartu kredit.




**Gambar 2. 4** Ilustrasi Serangan *Evil Twin*

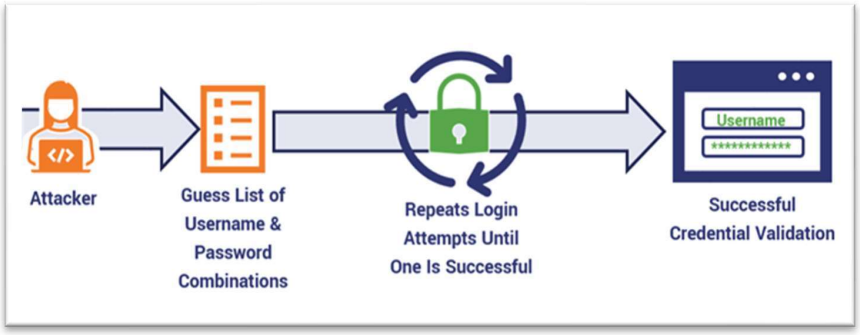
(Sumber : tuyensinh, 2025)

Serangan *Evil Twin* sering kali digunakan bersamaan dengan teknik lain seperti *phishing* atau *Man-in-the-Middle (MitM)* untuk meningkatkan efektivitasnya. Misalnya, setelah korban terhubung ke *access point* palsu, penyerang dapat menampilkan halaman *login* palsu yang tampak seperti halaman asli dari suatu layanan (misalnya *login WiFi* publik), dan memancing korban untuk memasukkan kredensial mereka. Karena serangan ini memanfaatkan kepercayaan pengguna terhadap jaringan yang tampaknya sah, sangat sulit bagi pengguna awam untuk menyadari bahwa

mereka sedang menjadi target. Oleh karena itu, penting untuk menggunakan jaringan yang aman dan menggunakan VPN saat terhubung ke WiFi publik.

4. *Bruteforce*

Salah satu cara serangan keamanan siber yang dikenal sebagai *bruteforce attack* adalah serangan yang menebak kombinasi kredensial, seperti *username* dan *password*, berulang kali hingga menemukan kombinasi yang tepat. Sampai berhasil mendapatkan akses ke sistem target, serangan ini mencoba berbagai kombinasi karakter, baik secara acak maupun berdasarkan pola tertentu.




**Gambar 2. 5** Ilustrasi Serangan *Bruteforce*

(**Sumber:** Mugila. Y, 2023)

Serangan *brute force* biasanya dilakukan secara otomatis menggunakan perangkat lunak khusus, dan dapat memakan waktu lama tergantung pada kompleksitas data yang dicoba. Serangan ini bisa sangat efektif jika sistem tidak memiliki perlindungan yang cukup, seperti pembatasan jumlah percobaan *login* atau penggunaan autentikasi dua faktor. Untuk mencegah *bruteforce*, sistem harus menerapkan pengamanan seperti penggunaan

*password* yang panjang dan kompleks, *CAPTCHA*, dan penguncian akun setelah beberapa kali percobaan gagal.(Hidayat & Ramli, 2023)

**2.1.3.2 Mitigasi**

Mitigasi merupakan langkah-langkah yang dilakukan untuk mengurangi dampak atau mencegah terjadinya serangan keamanan. Strategi mitigasi mencakup:

1. *Firewall*

   *Firewall* menyaring lalu lintas masuk dan keluar berdasarkan aturan keamanan tertentu untuk mencegah akses yang tidak sah. *Firewall* terutama jenis *Next-Generation Firewall (NGFW*) merupakan garis pertahanan utama dengan kemampuan inspeksi paket mendalam, kontrol aplikasi, dan *threat intelligence*. *NGFW* mampu mengenali lalu lintas per aplikasi dan memblokir ancaman tingkat lanjut serta *zero-day*, serta adaptif dan dapat diintegrasikan ke sistem *cloud modern*. (Bringhenti et al., 2024) mengusulkan *firewall reconfiguration* otomatis menggunakan *AI* untuk mendeteksi dan merespons ancaman secara *realtime.*

2. *Patch Management*

   Patch management merupakan proses sistematis dalam pengelolaan patch mulai dari identifikasi, akuisisi, pengujian, hingga instalasi untuk memperbaiki kerentanan yang dikenal, Proses pembaruan perangkat lunak dilakukan untuk menutup celah keamanan yang diketahui.

3. *Backup* dan *Recovery*

   *Backup* dan *recovery* merupakan strategi penting dalam mitigasi serangan siber, terutama dalam menghadapi ancaman seperti *ransomware*, kegagalan

sistem, maupun bencana alam. Proses pencadangan (backup) data secara berkala memungkinkan organisasi untuk memulihkan informasi penting yang hilang, rusak, atau dienkripsi oleh pelaku kejahatan siber. Penerapan strategi ini mencakup identifikasi data kritis yang perlu dicadangkan, pemilihan media penyimpanan (baik lokal, *cloud*, atau *hybrid*), serta penjadwalan pencadangan secara otomatis.(Taresh Mehra, 2024)

Menurut penelitian yang diterbitkan oleh (Thomas & Galligher, 2018) menyebut backup sebagai "barisan pertahanan terakhir" yang efektif memulihkan sistem ke status valid pra-serangan. Mereka merekomendasikan agar proses asesmen keamanan informasi secara eksplisit mengevaluasi kemampuan backup dalam menangani scenario *ransomware*.

Dengan sistem *backup* dan *recovery* yang baik, tidak hanya dapat meminimalkan kerugian akibat serangan siber, tetapi juga menjaga keberlangsungan operasional dan reputasi. Praktik terbaik juga merekomendasikan penggunaan enkripsi pada data cadangan serta pembatasan akses hanya kepada personel yang berwenang untuk mencegah penyalahgunaan atau kebocoran data.

### *2.1.4 Tools*

Dalam menganalisis dan menguji keamanan jaringan nirkabel, dibutuhkan serangkaian *tools* yang dirancang khusus untuk melakukan pemindaian, eksploitasi, dan pemantauan lalu lintas jaringan.. Penjelasan masing-masing *tools* akan diuraikan dalam subbab berikut.

### *2.1.4.1 Kali Linux*

*Kali Linux* merupakan distribusi *Linux open source* yang dirancang khusus untuk pengujian penetrasi (*penetration testing*) dan peretasan etis (*ethical hacking*). Ini adalah sistem operasi yang sangat populer di kalangan profesional keamanan siber, peneliti keamanan, dan penggemar etika hacking. Dikembangkan dan dikelola oleh *Offensive Security*, *Kali Linux* hadir dengan koleksi alat yang sangat besar dan komprehensif, memungkinkan pengguna untuk melakukan berbagai tugas terkait keamanan, mulai dari analisis kerentanan, forensik digital, hingga rekayasa balik.(Lu & Yu, 2021)


**Gambar 2. 6** Kali Linux

(**Sumber :** Pxfuel, n.d.)

Salah satu fitur paling menonjol dari *Kali Linux* adalah kelengkapan toolsetnya. Sistem operasi ini sudah terintegrasi dengan ratusan *tools* yang dikategorikan berdasarkan fungsinya, seperti pengumpulan informasi, analisis kerentanan, serangan *web application*, pengujian jaringan nirkabel, *password attacks*, dan banyak lagi. Kemudahan akses terhadap *tools* ini membuat *Kali Linux* menjadi pilihan utama bagi mereka yang ingin melakukan audit keamanan,

mengidentifikasi kelemahan dalam sistem, atau mensimulasikan serangan siber untuk menguji ketahanan sebuah infrastruktur IT.

Selain kelengkapan *tools*, *Kali Linux* juga dikenal karena fleksibilitas dan kemudahan penggunaannya. Meskipun awalnya mungkin terasa kompleks bagi pemula, komunitas yang besar dan dokumentasi yang ekstensif membuatnya relatif mudah untuk dipelajari. *Kali Linux* dapat diinstal di berbagai perangkat keras, termasuk komputer *desktop*, *laptop*, *server*, bahkan perangkat *ARM* seperti *Raspberry Pi*. Ini juga dapat dijalankan sebagai mesin *virtual* atau dari *USB drive* yang dapat di *boot* (*live USB*), memberikan fleksibilitas tinggi bagi pengguna untuk membawanya dan menggunakannya di mana saja. Tujuan utamanya adalah memberdayakan individu dan organisasi untuk secara proaktif mengidentifikasi dan memperbaiki celah keamanan sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab.

#### *2.1.4.2 Packet Tools Aircrack-ng*

*Aircrack-ng* merupakan suite perangkat lunak (*toolset*) yang bersifat *open source* yang dirancang khusus untuk mengaudit keamanan jaringan nirkabel (*Wifi*). Paket *tools* ini sangat populer di kalangan profesional keamanan siber, peneliti, dan *ethical hacker* untuk menguji kerentanan jaringan *WiFi*. Fungsi utamanya berfokus pada pemantauan, penyerangan, pengujian, dan peretasan jaringan nirkabel, menjadikannya alat yang tak tergantikan untuk menilai seberapa aman sebuah jaringan *Wifi*.

Di dalam paket *Aircrack-ng*, terdapat beberapa *tools* penting dengan fungsi spesifik. Misalnya, *Airmon-ng* digunakan untuk mengaktifkan *mode monitor* pada

kartu nirkabel, yang memungkinkan kartu tersebut menangkap semua lalu lintas nirkabel di sekitarnya. *Airodump-ng* berfungsi untuk menangkap paket-paket data dan mengidentifikasi jaringan-jaringan *Wi-Fi* yang ada, termasuk informasi penting seperti *SSID, BSSID*, dan saluran yang digunakan. Sementara itu, *Aireplay-ng* digunakan untuk menyuntikkan (*inject*) atau memutar ulang (*replay*) paket-paket ke dalam jaringan, yang sering kali dimanfaatkan untuk mempercepat proses penangkapan *handshake WPA/WPA2* atau untuk melakukan serangan *deauthentication* agar klien terputus dari jaringan.(Muhammad Farhan Fauzan & Agung Susilo Yuda Irawan, 2021)


**Gambar 2. 7** Aircrack-ng

(**Sumber :** mister_x, 2023)

Puncak dari suite ini adalah *Aircrack-ng* itu sendiri, yang merupakan alat utama untuk memecahkan (*cracking*) kata sandi enkripsi *WEP* dan *WPA/WPA2-PSK*. *Aircrack-ng* bekerja dengan menganalisis paket data yang telah ditangkap (terutama handshake *WPA/WPA2*) dan mencoba menebak kata sandi menggunakan berbagai metode, seperti serangan kamus (dictionary attack) atau serangan brute-force. Dengan kombinasi tools ini, Aircrack-ng memungkinkan pengguna untuk secara proaktif menguji kekuatan keamanan kata sandi Wi-Fi dan mengidentifikasi potensi kerentanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung

jawab, sehingga membantu meningkatkan postur keamanan jaringan nirkabel secara keseluruhan.

Setiap tool di dalamnya memiliki peran spesifik yang saling melengkapi untuk membantu proses audit keamanan *Wi-Fi*. Berikut adalah beberapa tools utama dalam paket *Aircrack-ng*.

1. *Airmon-ng*

   *Airmon-ng* adalah *tool* pertama yang biasanya digunakan dalam alur pengujian keamanan nirkabel dengan *Aircrack-ng*. Fungsinya adalah untuk mengaktifkan mode monitor pada *wireless network interface card*. Dalam mode normal, kartu jaringan hanya mendengarkan lalu lintas yang ditujukan kepadanya. Namun, dengan mode *monitor*, kartu jaringan dapat menangkap semua paket data yang melayang di udara dalam jangkauannya, terlepas dari apakah paket tersebut ditujukan atau tidak. Ini adalah langkah krusial untuk bisa mengumpulkan data dari jaringan Wi-Fi target.

2. *Airodump-ng*

   Setelah *wireless card* berada dalam *mode monitor* berkat *Airmon-ng*, giliran *Airodump-ng* yang berperan. *Airodump-ng* adalah penangkap paket (*packet sniffer*) dan pemindai (*scanner*) yang digunakan untuk mendeteksi jaringan-jaringan *Wi-Fi* di sekitar, mengumpulkan informasi tentangnya, dan menangkap paket data. Informasi yang dikumpulkan mencakup *SSID* (nama jaringan), *BSSID* (alamat *MAC access point*), saluran (*channel*), jenis enkripsi (*WEP, WPA, WPA2*), dan bahkan daftar klien yang terhubung ke *access point* tertentu. *Airodump-ng* juga sangat penting untuk menangkap "*handshake*"

*WPA/WPA2*, yang merupakan momen krusial saat klien terhubung ke jaringan dan menjadi target utama untuk peretasan kata sandi.

3. *Aireplay-ng*

   *Aireplay-ng* adalah *tool* yang berfungsi untuk menyuntikkan (*inject*) dan memutar ulang (*replay*) paket-paket ke dalam jaringan nirkabel. Ini digunakan untuk tujuan aktif seperti mempercepat pengumpulan *IVs (Initialization Vectors*) pada jaringan *WEP*, atau untuk memaksa terjadinya *handshake WPA/WPA2*. Salah satu serangan populer yang dilakukan dengan *Aireplay-ng* adalah serangan *deauthentication*, di mana klien yang sah akan diputus dari jaringan, dan ketika mereka mencoba menyambung kembali, *handshake WPA/WPA2* dapat ditangkap oleh *Airodump*-ng. Selain itu, *Aireplay-ng* juga dapat digunakan untuk berbagai jenis serangan lain, seperti *ARP request injection* untuk menghasilkan lebih banyak lalu lintas.

4. *Aircrack-ng*

   Ini adalah *tool* inti atau *cracker* utama dalam *suite Aircrack-ng*. Setelah paket data yang relevan (terutama *handshake WPA/WPA2* atau *IVs WEP*) berhasil ditangkap oleh *Airodump-ng, Aircrack-ng* akan mencoba untuk memecahkan kata sandi jaringan. Untuk enkripsi *WEP*, *Aircrack-ng* menggunakan serangan statistik berdasarkan *IVs* yang dikumpulkan. Sementara untuk *WPA/WPA2-PSK*, *Aircrack-ng* bekerja dengan membandingkan *hash* dari *handshake* yang ditangkap dengan hash yang dihasilkan dari daftar kata sandi (*Wordlists*) atau mencoba semua kemungkinan kombinasi karakter

(*bruteforce*). Keberhasilan peretasan sangat bergantung pada kekuatan kata sandi dan kelengkapan wordlist yang digunakan.

5. *Airbase-ng*

   *Airbase-ng* adalah tool yang dapat digunakan untuk membuat *access point palsu* (*evil twin*) atau untuk melakukan serangan terhadap klien daripada hanya *access point*. Ini memungkinkan penyerang untuk meniru sebuah jaringan *Wi-Fi* yang sah, menunggu klien yang sebelumnya terhubung untuk mencoba menyambung kembali secara otomatis. Setelah klien terhubung ke AP palsu ini, penyerang dapat mencegat lalu lintas, mengumpulkan *IVs*, atau bahkan melakukan serangan *man-in-the-middle*. *Airbase-ng* juga memiliki kemampuan untuk melakukan serangan spesifik seperti *Caffe Latte attack* dan *Hirte attack*.

6. *Airdecap-ng*

   *Airdecap-ng* merupakan alat yang digunakan untuk mendekripsi berkas tangkapan (*capture files*) yang menggunakan enkripsi *WEP/WPA/WPA2*. Setelah kata sandi jaringan berhasil diperoleh, jika paket yang ditangkap masih terenskripsi, *Airdecap-ng* dapat digunakan untuk mendekripsi data tersebut. Dengan demikian, alat ini memungkinkan analisis lalu lintas jaringan yang sebelumnya terenkripsi, yang sangat berguna dalam analisis forensik atau untuk mempelajari data yang melewati jaringan setelah kunci berhasil diperoleh.

7. *Packetforge-ng*

*Packetforge-ng* adalah tool yang dirancang untuk membuat paket-paket terenkripsi khusus yang dapat disuntikkan ke dalam jaringan. Tool ini sangat berguna untuk membuat berbagai jenis paket (seperti paket *ARP request*) yang kemudian dapat digunakan oleh *Aireplay-ng* untuk tujuan injeksi. Dengan membuat paket-paket yang dimanipulasi ini, *Packetforge-ng* membantu dalam mempercepat proses pengumpulan data yang diperlukan untuk peretasan kata sandi *WEP* atau untuk memicu respons tertentu dari jaringan.

#### *2.1.4.3 Wireshark*

*Wireshark* merupakan sebuah perangkat lunak open-source yang digunakan untuk menangkap dan menganalisis paket data dalam jaringan komputer. Perangkat ini berfungsi sebagai packet *analyzer* atau *network sniffer* yang memungkinkan pengguna untuk memantau lalu lintas data secara *realtime* maupun melalui file hasil tangkapan sebelumnya. *Wireshark* mampu mendekode dan menampilkan berbagai jenis protokol jaringan, seperti *TCP, UDP, HTTP, DNS*, dan lainnya dalam format yang terstruktur dan mudah dianalisis. Dengan antarmuka yang interaktif serta fitur *filter* yang canggih, *Wireshark* menjadi alat yang sangat bermanfaat dalam proses *troubleshooting* jaringan, pemantauan performa, analisis keamanan, maupun pengembangan sistem komunikasi berbasis jaringan. Karena sifatnya yang lintas *platform* dan bersifat gratis, *Wireshark* banyak digunakan oleh profesional TI, peneliti, pengembang, hingga mahasiswa dalam memahami dan mengelola trafik jaringan secara lebih mendalam dan akurat. (Mala et al., 2023)

## 2.2 Penelitian Terdahulu

Penelitian terdahulu digunakan sebagai dasar untuk memperkuat landasan teori dan menunjukkan adanya relevansi serta keterkaitan antara penelitian yang dilakukan dengan penelitian yang sudah ada sebelumnya.

1. penelitian (Adiguna & Widagdo, 2022) dengan judul "analisis keamanan jaringan wpa2-psk menggunakan metode *penetration testing* (Studi Kasus : *Router TP-Link Mercusys Mw302r*)", menurut peneliti Ketika data berpindah melalui jaringan dari satu titik ke titik lain, ada risiko bahwa pihak yang tidak berwenang dapat mengubah atau menyadap informasi tersebut. Ini berarti setiap kali data dikirimkan, ada potensi bagi individu yang berniat jahat untuk mencegat dan memanipulasi isinya sebelum mencapai tujuan akhir. Merancang sistem keamanan untuk jaringan *WLAN (Wireless Local Area Network*) yang terhubung ke internet adalah hal yang krusial. Proses ini memerlukan pemahaman mendalam dan perencanaan yang matang untuk memastikan data terlindungi dari ancaman siber.
2. Penelitian (Anam & Fachri, 2025) yang berjudul "Evaluasi Kerentanan Keamanan Jaringan Nirkabel Menggunakan Metode *Penetration Testing* Dengan *Aircrack-Ng*", menurut peneliti Banyak jaringan nirkabel masih rentan terhadap serangan karena tetap menggunakan pengaturan bawaan atau default. Penggunaan pengaturan standar ini secara signifikan membuka celah keamanan, mempermudah pihak tidak bertanggung jawab untuk mengakses atau mengeksploitasi jaringan tersebut. Maka dari itu Sangatlah penting untuk memahami sistem keamanan jaringan nirkabel yang kita gunakan dan seberapa

baik jaringan tersebut bisa bertahan dari ancaman eksternal. Salah satu cara paling efektif untuk menguji ketahanan ini adalah dengan melakukan *penetration testing*.

3. Penelitian (Arini, n.d.) dengan judul *"Pengujian Celah Keamanan 5 Jenis Metode Wireless LAN Security"*, menurut peneliti, sistem keamanan jaringan wireless memiliki kelemahan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk mengakses data secara ilegal. Dalam studi ini, lima metode keamanan *WLAN* yaitu *WEP*, *WPA/WPA2*, *MAC Filtering*, *Hidden SSID*, dan *WPA2-RADIUS* diuji menggunakan berbagai *tools opensource* untuk mengevaluasi efektivitas perlindungannya. Hasil pengujian menunjukkan bahwa *WEP* sangat rentan terhadap cracking. Sebaliknya, *WPA/WPA2* dan *WPA2-RADIUS* terbukti lebih tangguh, meskipun efektivitasnya tetap bergantung pada konfigurasi sistem dan kekuatan kata sandi yang digunakan. Peneliti menekankan bahwa pemilihan metode keamanan yang tepat, dikombinasikan dengan pengaturan konfigurasi yang kuat, sangat penting untuk meminimalisasi risiko kebocoran data. Oleh karena itu, pengawasan rutin dan penerapan protokol keamanan yang mutakhir menjadi langkah krusial dalam memperkuat pertahanan jaringan *WLAN* dari berbagai bentuk serangan.
4. Penelitian (Yusnanto et al., 2022) dengan judul *"Analisa Infrastruktur Jaringan Wireless (WLAN) menggunakan Wireshark dan Penetration Testing Kali Linux"*, menurut peneliti, keamanan jaringan nirkabel sangat rentan terhadap berbagai jenis serangan yang memanfaatkan celah pada komunikasi data, seperti *sniffing dan spoofing*. Dalam studi ini, penggunaan *Kali Linux* dan *Wireshark*

sebagai alat bantu analisis memungkinkan peneliti mengidentifikasi pola lalu lintas jaringan serta mendeteksi potensi celah keamanan secara langsung di lapangan. Peneliti menekankan bahwa pemantauan aktivitas jaringan secara real-time dan penerapan metode *penetration testing* sangat penting untuk mengetahui seberapa besar risiko kebocoran data yang mungkin terjadi. Maka dari itu, dibutuhkan konfigurasi keamanan yang tepat serta pengawasan berkelanjutan terhadap sistem jaringan wireless agar lebih tahan terhadap ancaman siber.

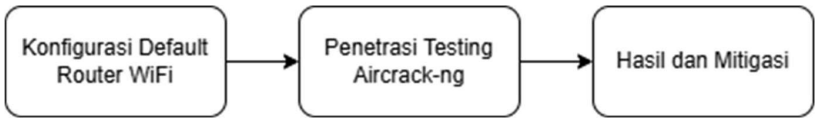
5. Penelitian (Fajri et al., 2019) dengan judul *"Studi Empiris terhadap Kinerja & Keamanan WiFi (Studi Kasus di Kota Depok)"*, menurut peneliti, jaringan nirkabel yang tersebar di wilayah perkotaan seperti Kota Depok masih menghadapi berbagai potensi risiko keamanan, terutama pada jaringan yang menggunakan enkripsi lama atau bahkan tidak menggunakan proteksi sama sekali. Dalam studi ini, peneliti melakukan pemindaian terhadap ratusan jaringan WiFi menggunakan metode *wardriving*, dan menemukan bahwa sebagian besar jaringan telah menggunakan protokol *WPA/WPA2*, namun masih ada jaringan yang terbuka atau menggunakan *WEP* yang rentan terhadap serangan. Peneliti juga menganalisis penggunaan kanal jaringan dan menemukan bahwa sebagian besar jaringan mengikuti standar kanal optimal (1, 6, dan 11) untuk meminimalkan interferensi. Studi ini menekankan pentingnya konfigurasi keamanan yang kuat, penggunaan protokol enkripsi modern, dan kesadaran pengguna terhadap risiko yang dapat timbul dari penggunaan jaringan yang tidak aman. Oleh karena itu, dibutuhkan upaya sistematis untuk meningkatkan

keamanan dan performa jaringan WiFi di lingkungan publik melalui edukasi dan penegakan standar teknis.

6. Penelitian (Ernawati et al., 2024) yang berjudul *"Case Study in Network Security System Using Random Port Knocking Method on The Principles of Availability, Confidentiality and Integrity"* membahas penerapan metode keamanan jaringan menggunakan *Random Port Knocking* (RPK) untuk menjaga prinsip-prinsip ketersediaan, kerahasiaan, dan integritas. Studi ini dilakukan pada sistem berbasis *Debian* dan memanfaatkan *tools* seperti *Nmap* dan *Hydra* untuk menguji ketahanan terhadap serangan *port scanning*. Hasil menunjukkan bahwa metode ini mampu mencapai *availability* sebesar 99,97%, menjaga *confidentiality* 100%, serta memiliki waktu respon rata-rata 0,22 detik dengan tingkat akurasi pemblokiran 100%. Penelitian ini menegaskan bahwa RPK dapat menjadi solusi efektif dalam melindungi *port* layanan *server* dari akses yang tidak sah, selama dikonfigurasi dan dipantau dengan baik.
7. Penelitian (Kolev & Shterev, 2024) yang berjudul "*Wireless Security Issues*" membahas isu keamanan jaringan *wireless* eksperimental. Tools seperti *airmon-ng* dan *aircrack-ng* digunakan untuk menganalisis lalu lintas jaringan dan mengidentifikasi celah keamanan. Hasil menunjukkan bahwa deteksi dini terhadap ancaman bisa dilakukan jika konfigurasi jaringan diperiksa secara berkala, Penelitian ini mengevaluasi performa *aircrack-ng* dalam memecahkan kata sandi *WiFi*. Ditemukan bahwa efektivitas sangat tergantung pada kekuatan password dan jenis enkripsi.

8. Penelitian (Antaryami, 2021) yang berjudul "*Comparative Analysis of Parrot, Kali Linux and Network Security Toolkit (NST)*" menganalisis perbandingan distribusi *Linux* untuk keamanan jaringan. *Aircrack-ng* dipakai untuk menguji kekuatan *WiFi* di tiap platform. Hasilnya menunjukkan *Kali Linux* memiliki integrasi *tools* keamanan terbaik dalam hal stabilitas dan kompatibilitas *driver wireless*.
9. Penelitian (Asaad, 2021) berjudul "*Penetration Testing: Wireless Network Attacks Method on Kali Linux OS*" membahas teknik serangan berbasis *Kali Linux* dengan *aircrack-ng*, termasuk *injection* dan *packet replay*. Penelitian ini menunjukkan bahwa *WiFi* publik sangat rentan terhadap *sniffing* jika tidak menggunakan protokol yang kuat seperti *WPA3*

## 2.3 Kerangka Pemikiran




**Gambar 2. 8** Kerangka Pemikiran
(**Sumber :** Data Penelitian 2025)

Tahap awal dimulai dengan menggunakan pengaturan *default* pada *router WiFi*, dan konfigurasi keamanan yang belum dimodifikasi. Penggunaan konfigurasi default ini bertujuan untuk mensimulasikan kondisi umum yang sering ditemukan pada jaringan WiFi pengguna rumahan atau kantor kecil, yang sering kali menjadi target serangan karena pengamanannya yang masih lemah.

Selanjutnya, dilakukan pengujian penetrasi terhadap jaringan WiFi menggunakan *tools Aircrack-ng* yang dijalankan melalui sistem operasi *Kali Linux*. Pengujian ini melibatkan tahapan seperti pemindaian *SSID* target, proses capturing *handshake*, hingga proses *cracking* kata sandi menggunakan metode *brute force* atau *dictionary attack*.

Tahap Selanjutnya bertujuan untuk mengidentifikasi kelemahan autentikasi dan enkripsi yang digunakan dalam jaringan. Setelah proses pengujian selesai, dilakukan analisis terhadap hasil penetrasi untuk menentukan tingkat kerentanan jaringan. Berdasarkan temuan tersebut, dirumuskan strategi mitigasi yang relevan, seperti menonaktifkan fitur *WPS*, mengganti sandi dengan kombinasi kompleks, serta mengaktifkan fitur keamanan lanjutan pada router. Mitigasi ini bertujuan untuk memperkuat keamanan jaringan WiFi dan mencegah terjadinya serangan serupa di masa mendatang.