Implementasi Wireless Intrusion Detection System Untuk Mendeteksi Keberadaan Access Point Untuk Area No Signal Policy

1st Dinda Chairunnisa Putri
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
dindachaaa@telkomuniversity.ac.id

2nd Ida Wahidah Hamzah
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
wahidah@telkomuniversity.ac.id

3rd Fardan
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
fardanfnn@telkomuniversity.ac.id

***Abstrak* — Wireless Intrusion Detection System atau yang disingkat dengan Wireless IDS adalah sebuah sistem yang digunakan untuk mendeteksi aktivitas yang mungkin akan merugikan sebuah suatu sitem nirkabel, salah satunya adalah untuk mendeteksi keberadaan access point berupa jaringan Wi-Fi. Sistem ini dibuat dengan memanfaatkan sistem operasi Kali-Linux menggunakan aturan dan pola-pola bawaan untuk mengenali tanda-tanda yang mencurigakan. Wireless IDS ini berperan penting dalam menjaga keamanan jaringan nirkabel di lingkungan yang rentan dan membutuhkan sebuah keamanan dari serangan atau intrusi. Dengan mmenggunakan sistem ini secara berkala, Wireless IDS dapat mencegah potensi risiko dan kerentanan keamanan yang dapat merugikan integritas dan kerahasiaan data.**

***Kata kunci*— Wireless Intrusion Detection System, No Signal Policy, Access Point Wi-Fi, Keamanan Jaringan Nirkabel**

I. PENDAHULUAN

Penggunaan jaringan nirkabel, terutama melalui access point Wi-Fi, menjadi sebuah ketergantungan pada konektivitas jaringan nirkabel. Oleh sebab itu, pada suatu instasi atau perusahaan menerapkan kebijakan area no signal policy, hal ini merupakan sebuah perlindungan dari ancaman untuk keamanan integritas data. No signal policy disini dimaksudkan dimana akses Wi-Fi seharusnya tidak ada. Dengan demikian, kebijakan ini memberikan area yang bebas dari potensi risiko dan ancaman melalui jaringan nirkabel.

Penelitian akan sistem implementasi Wireless IDS ini berguna untuk pengenalan karakteristik sinyal Wi-Fi yang tidak sah, integrasi sistem berupa kecerdasan buatan dalam mengidentifikasi informasi parameter Wi-Fi diharapkan dapat meningkatkan efisiensi dan mengetahui jarak keberadaan Wi-Fi dalam radius tertentu.

II. KAJIAN TEORI

A. Wireless Intrusion Detection System (Wireless IDS)

Wireless IDS adalah langkah-langkah yang sangat penting dalam memitigasi risiko kemananan dalam jaringan nirkabel. Disini, IDS memiliki peran untuk menyajikan informasi yang dibutuhkan dalam menganalisis parameter-parameter Wi-Fi. Dengan mengamati hasil parameter-parameter Wi-Fi terdeteksi, penelitian ini memiliki pertimbangan dan batasan akan ketidakpastian jarak.

B. TP-Link WN725N

Perangkat keras TP-Link WN725N, yang merupakan USB *wireless adapter*, digunakan untuk mendeteksi sinyal *Wi-Fi* yang ada di sekitarnya. Perangkat ini menggunakan antena untuk menangkap gelombang radio yang dipancarkan oleh jaringan *Wi-Fi.* TP-Link WN725N dihubungkan ke komputer yang menjalankan sistem operasi Kali-Linux melalui port USB. Kali-Linux adalah sistem operasi yang sering digunakan untuk keperluan keamanan dan pengujian jaringan, termasuk pengujian *Wi-Fi.*

B. Sistem Operasi Kali-Linux

Sistem operasi Kali-Linux adalah sistem yang digunakan untuk menjaga keamanan yaitu salah satunya keamanan jaringan, Kali-Linux merupakan sistem operasi yang bersifat open-source. Kali-Linux menyediakan beberapa alat kemanan siber yang dapat menampilkan enkripsi dan analisis suatu jaringan yang bisa ditampilkan pada antarmuka grafis (GUI). Di dalam Kali Linux, airodump-ng untuk me-*monitor* dan menangkap sinyal *Wi-Fi* yang dideteksi oleh TP-Link WN725N.

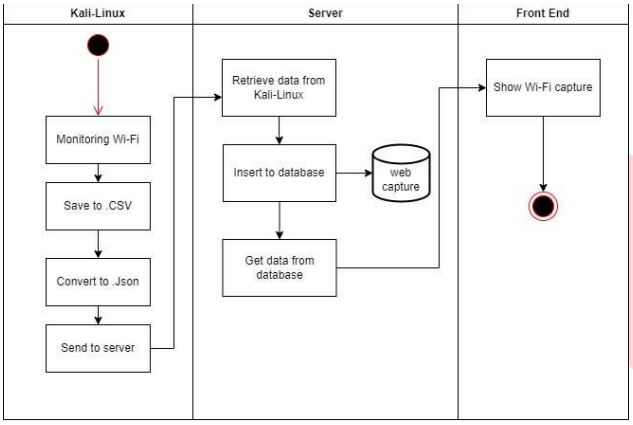
Integrasi dari Kali-Linux ke airodump-ng digunakan untuk menganalisis jaringan Wi-Fi. Dengan menggunakan airodump-ng pengguna dapat mengumpulkan dan menganalisis paket data yang dikirimkan melalui jaringan nirkabel. Dengan mengubah antarmuka nirkabel menjadi mode pemantauan, sistem dapat menampilkan lalu lintas jaringan secara pasif saat terhubung ke jaringan. Enkripsi WEP atau WPA/WPA2 dapat dipecahkan jika kata sandi terindikasi lemah. Data-data parameter Wi-Fi disimpan dalam bentuk .csv yang diubah ke.json dan dikirimkan ke antarmuka GUI dengan memanfaatkan hostinger untuk mode web monitor.

III. METODE

Berikut ini adalah gambaran rancangan penelitian analisis jarak Wi-Fi berdasarkan daya sinyal (power) untuk mendeteksi keberadaan access point Wi-Fi yang tidak sah:

A. Perancangan Sistem

Perancangan sistem yang digunakan untuk menganalisis parameter-parameter Wi-Fi yang terdeteksi bertujuan untuk mengambil dataset yang diperlukan untuk melakukan pengolahan data. Dapat dilihat pada gambar berikut cara kerjanya:



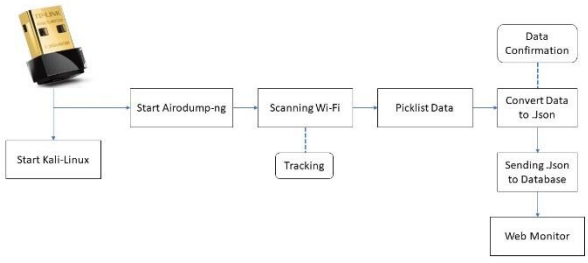
GAMBAR 3.1
Rancangan sistem deteksi Wi-Fi

Pada gambar tersebut, terlihat rancangan sistem untuk deteksi Wi-Fi saat pengambilan dataset parameter Wi-Fi pada Kali-Linux. Sistem ini diintegrasikan pada airodump-ng meliputi penerimaan, mengonversi dan mengirim dataset ke web capture. Berikut penjelasan dari flowchart diatas:

1. Mendeteksi keberadaan jaringan Wi-Fi dan data parameter Wi-Fi disimpan dalam bentuk file .csv
2. Mengkonversi file .csv Wi-Fi ke file .json agar database dapat diterima oleh server
3. Data yang sudah diambil oleh Aircrack-ng pada Kali-Linux ditangkap dan dimasukkan ke dalam database dan ditampilkan pada web monitor

B. Desain Simulasi

Gambar dibawah merupakan model dari sistem yang akan dilakukan untuk pengujian pendeteksi jaringan Wi-Fi.



GAMBAR 3.2
Skema infrastruktur deteksi Wi-Fi

Penulis akan membangun sebuah infastruktur pendeteksian Wi-Fi yang memiliki komponen berupa Kali-Linux dan airodump-ng. Informasi yang terkumpul akan ditampilkan pada antarmuka airodump-ng di Kali-Linux. Antarmuka ini menyajikan data dalam bentuk tabel yang terus diperbarui secara *real time* untuk mencerminkan perubahan pada sinyal *Wi-Fi* yang terdeteksi.

Platform infrastruktur yang sudah berhasil dirancang akan digunakan untuk menampilkan informasi yang didapatkan berupa parameter Wi-Fi mencakup alamat BSSID, daya sinyal *(power)*, jumlah *beacon (beacons),* jumlah data (#data), kecepatan pengiriman (#/s), saluran *(channel),* mode transmisi (MB), enkripsi *(encryption)*, algoritma kriptografi *(chiper),* metode autentikasi *(authentication),* nama SSID (essid), daya sinyal stasiun terkait *(station power),* kecepatan transmisi *(rate),* jumlah paket yang hilang *(lost),* jumlah frame yang hilang *(frames)*, catatan *(notes)*, dan sinyal probe *(probes).* Berikut adalah perintah untuk menamoilkan parameter Wi-Fi.

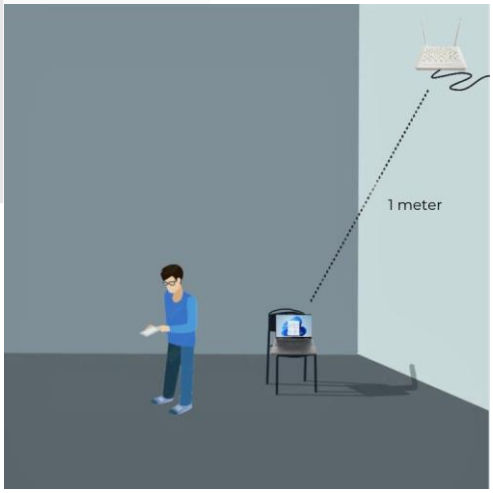
```
sudo airodump-ng wlan0 -w –write-interval 5 -0 csv
```

Untuk perintah yang dijalankan untuk menganalisis salah satu jaringan Wi-Fi dengan opsi real time per 5 detik dalam bentuk file .csv.

IV. HASIL DAN PEMBAHASAN

A. Pengujian Fungsionalitas Sistem

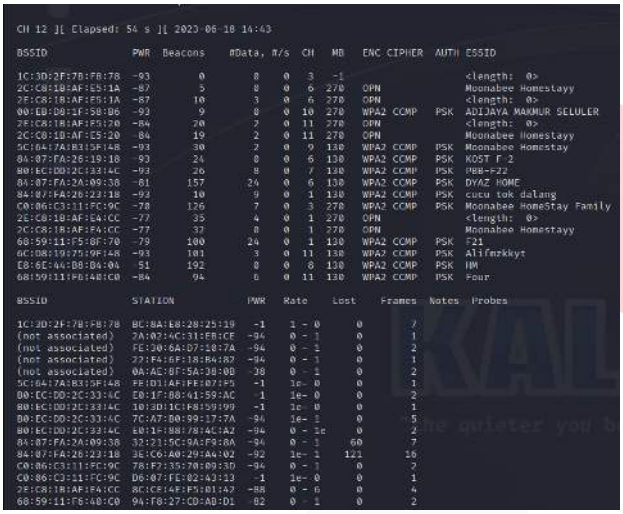
Pengujian fungsionalitas dilakukan untuk memastikan bahwa sistem yang dirancang berfungsi dengan baik. Pengujian ini bisa dikatakan berhasil jika data parameter Wi-Fi yaitu daya sinyal (power) tidak terjadi anomali. Simulasi pengujian sistem dijalankan pada PC sebagai monitor dan router sebagai access point. Langkah awal yang harus dilakukan yaitu memastikan TP-Link WN725N dapat menangkap dataset parameter Wi-Fi yang ditampilkan pada sistem operasi Kali-Linux. Dan diintegrasikan ke airodump-ng. Sebelum menggunakan airodump-ng, TP-Link WN725N perlu dikonfigurasi ke dalam mode monitor. Mode monitor memungkinkan perangkat untuk menangkap dan menganalisis semua paket yang dikirimkan melalui jaringan *Wi-Fi,* bukan hanya paket yang ditujukan untuk perangkat tersebut. Melakukan pemindahan jarak per satu meter dan mengamati nilai daya sinyal (power).



GAMBAR 4.1
Ilustrasi saat pengujian wifi

Pada Gambar 4.1 merupakan ilustrasi pengujian *Wi-Fi* di dalam ruangan tanpa pembatas (LOS) yang terdapat *router*

sebagai *access point.* Pengujiannya dilakukan dengan cara memindahkan perangkat yang terhubung ke jaringan *Wi-Fi* per satu meter ke depan atau ke belakang, dan perhatikan perubahan pada nilai power yang ditampilkan oleh airodump-ng. Pengukuran ini dilakukan selama 10 kali percobaan dalam rentang satu menit dalam rentang waktu yang berbeda dengan jarak per satu meter. Lalu hasil dari nilai sinyal daya (power) dicatat agar dapat mengidentifikasi pola perubahan nilainya. Dengan begitu, kita dapat melakukan analisa yang lebih baik tentang kekuatan sinyal Wi-Fi di area pengujian. Pengujian sistem dapat berjalan dengan baik seperti gambar di bawah.



GAMBAR 4.2
Hasil deteksi Wi-Fi

Pada gambar diatas dapat terlihat bahwa sistem pendeteksian Wi-Fi dapat berjalan dengan baik. Langkah selanjutnya diperlukan pemilahan data (picklist) untuk menganalisis jaringan Wi-Fi karena hanya beberapa data yang diperlukan dan beberapa data lainnya yang dilarang karena alasan privasi.

GAMBAR 4.3
Picklist parameter Wi-Fi

Pada gambar 4.3 merupakan hasil data yang sudah dipilah. Data yang dipilah mencakup BSSID, *Chiper, Power, Privacy, Last time seen, beacons,* dan ESSID. Tak hanya itu, pengguna dapat menjalankan script python dengan perintah "skrip_covert.py" untuk mendapatkan data tambahan, seperti menghitung jarak dari perangkat ke access point Wi-Fi dalam radius tertentu.

Hasil pengujiannya akan bergantung pada lingkungan pengujian dan kondisi yang spesifik. Hasil yang didapatkan dari pengujian ini adalah:

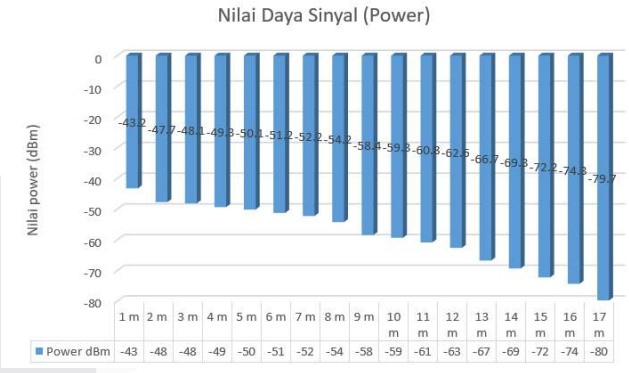
1. TP-Link WN725N dapat mendeteksi jaringan *Wi-Fi* yang ada di sekitarnya.
2. Informasi yang ditampilkan pada antarmuka airodump-ng tampil secara secara real time.
3. Sistem dapat bekerja dengan responsif selama pengujian yang dilakukan.
4. TP-Link WN725N kompatibel dengan sistem operasi Kali-Linux dan dapat berintegrasi dengan baik dengan airodump-ng.
5. Pemilahan data akan diupload ke web monitor. Dengan melakukan pengujian yang komprehensif terhadap hasil implementasi, Selanjutnya, kami dapat mengevaluasi kinerja sub-sistem secara keseluruhan dan mengidentifikasi kemungkinan perbaikan atau peningkatan yang diperlukan untuk meningkatkan fungsionalitas dan kehandalan sub-sistem deteksi Wi-Fi. Berikut merupakan tabel hasil nilai daya sinyal (power) yang telah diuji:

TABEL 4.1
Nilai power Wi-Fi yang diuji

Radius / Jarak	Pengujian ke-										Rata-Rata Nilai Power (dBm)
	1	2	3	4	5	6	7	8	9	10	
1 Meter	-47	-42	-44	-48	-43	-44	-45	-40	-41	-38	-43.2
2 Meter	-46	-44	-47	-50	-49	-48	-49	-50	-48	-46	-47.7
3 Meter	-50	-48	-45	-46	-48	-53	-50	-49	-45	-47	-48.1
4 Meter	-46	-49	-40	-41	-42	-45	-44	-50	-49	-87	-49.3
5 Meter	-53	-48	-48	-52	-49	-50	-49	-53	-49	-50	-50.1
6 Meter	-53	-49	-47	-49	-49	-51	-52	-55	-55	-52	-51.2
7 Meter	-54	-65	-50	-55	-52	-45	-46	-54	-49	-52	-52.2
8 Meter	-50	-52	-46	-55	-49	-47	-55	-63	-63	-62	-54.2
9 Meter	-62	-64	-61	-59	-61	-51	-50	-50	-65	-61	-58.4
10 Meter	-62	-60	-58	-55	-62	-59	-55	-60	-67	-55	-59.3
11 Meter	-62	-58	-63	-60	-65	-62	-56	-57	-63	-62	-60.8
12 Meter	-64	-65	-59	-65	-64	-61	-66	-60	-60	-62	-62.6
13 Meter	-65	-64	-73	-70	-60	-61	-68	-71	-69	-66	-66.7
14 Meter	-65	-69	-67	-68	-65	-68	-73	-75	-66	-77	-69.3
15 Meter	-75	-69	-66	-69	-70	-75	-79	-79	-69	-71	-72.2
16 Meter	-72	-77	-70	-72	-68	-69	-78	-81	-80	-76	-74.3
17 Meter	-81	-78	-76	-80	-81	-78	-84	-85	-82	-72	-79.7

B. Analisis Hasil

Setelah menyelesaikan pengujian, kita dapat menganalisis data yang telah dikumpulkan untuk melihat bagaimana nilai power berubah seiring dengan jarak dari router Wi-Fi. Berikut chart hasil tabel 4.1.



GAMBAR 4.4
Chart sinyal daya (power) Wi-Fi yang diuji

Berdasarkan pengujian yang telah dilakukan menggunakan router di dalam ruangan tanpa pembatas (LOS), didapatkan nilai sinyal daya (power) yang tidak konstan. Pada jarak 1-17 meter nilai sinyal daya (power) semakin meningkat setiap perpindahan jarak per satu meter dalam rentang waktu yang berbeda. Penurunan kekuatan sinyal ini terjadi karena sinyal Wi-Fi mengalami redaman dan penyebaran saat merambat melalui udara hambatan dari objek dan dinding di sekitarnya. Secara teknis, semakin jauh jaraknya dari titik akses, kekuatan sinyal yang diterima oleh perangkat penerima akan menurun. Artinya, nilai dBm akan meningkat menjadi lebih negatif. Nilai rata-rata cukup

dengan menjumlahkan semua nilai daya sinyal (power) dan dibagi 17 kali percobaan. Berikut rumus menghitung rata-rata nilai daya sinyal (power) yang sudah didapatkan.

$$\bar{x} = \frac{Nilai\ sinyal\ daya\ percobaan\ 1 + 2 + 3\ \ldots dst}{Jumlah\ Pengujian\ Wi - Fi\ yang\ dilakukan}$$

Pada jarak 1 meter kekuatan sinyal adalah -43.2 dBm, maka pada jarak yang lebih jauh seperti 17 meter, kekuatan sinyal biasanya akan lebih rendah, yaitu -79.7 dBm. Jadi, semakin jauh jaraknya dari titik akses, semakin rendah nilai dBm atau lebih negatif kekuatan sinyal yang diterima oleh perangkat penerima.

V. KESIMPULAN

Berdasarkan hasil pengujian yang sudah dilakukan, dapat diperoleh kesimpulan yaitu alat dapat mendeteksi jaringan Wi-Fi. Pada pengujian menggunakan router di dalam ruangan tanpa pembatas (LOS) menunjukkan kekuatan sinyal Wi-Fi tidak konstan dengan peningkatan jarak. Nilai dBm semakin negatif seiring jarak meningkat. Faktor seperti redaman ruang udara, redaman dinding dan objek, interferensi, dan pengaruh lingkungan mempengaruhi hasil pengujian. Meskipun hukum invers kuadrat berlaku, penurunan kekuatan sinyal tidak selalu sesuai prediksi.

Secara keseluruhan, semakin jauh dari titik akses, semakin rendah nilai dBm atau kekuatan sinyal yang diterima perangkat penerima, dipengaruhi oleh berbagai faktor kompleks. Dan untuk pengujiannya dapat dilakukan dengan pengujian prediktif menggunakan sebuah regresi linear untuk membandingkan data yang direkam dengan data yang sudah teridentifikasi. Hasil pengujian mengungkapkan bahwa sistem berhasil mendeteksi jaringan Wi-Fi dengan memberikan informasi yang relevan. Pada uji coba jaringan Wi-Fi, fluktuasi sinyal terpengaruh oleh berbagai faktor lingkungan. Meskipun demikian, untuk peneliti selanjutnya dapat menerapkan regresi linear dalam analisis dan optimasi jaringan nirkabel masih dapat dieksplorasi lebih lanjut. Deteksi jaringan dengan potensi tambahan melalui penerapan analisis regresi linear yang lebih mendalam yang ingin mengembangkan sistem Wireless IDS untuk pendeteksian Wi-Fi ini. Perlu diingat implementasi sistem ini tidak disarankan untuk disalahgunakan agar kerahasian data tetap terjaga dan peneliti tidak bertanggung jawab untuk segala tindak kejahatan yang dilakukan.

REFERENSI

[1] S. Boob and P. Jadhav, “Wireless Intrusion Detection System,” *Int J Comput Appl*, vol. 5, no. 8, pp. 9–13, Aug. 2010, doi: 10.5120/934-1312.

[2] H. Yang and F. Wang, “Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network,” *IEEE Access*, vol. 7, pp. 64366–64374, 2019, doi: 10.1109/ACCESS.2019.2917299.

[3] Airodump-ng, (last edited 2022, 5 Januari). mister_x. Diakses pada 8 Juni 2023 dari https://www.aircrack-ng.org/doku.php?id=airodump-ng

[4] Wireless Intrusion Detection System: Bastille, dari https://www.bastille.net/product/govt-wireless-intrusion-detection-system-wids