Implementasi *Tools Aircrack-ng* Untuk Menganalisis Keamanan Jaringan *Wifi* Menggunakan *Kali linux*

Aircrack-ng Tool Implementation for Wifi Network Security Analysis using Kali linux

Alief Achmad Fadzri[1)], Andi Maslan[2)]
[1,2]Teknik Informatika, fakultas Teknik dan Komputer, Universitas Putera Batam
Jalan R. Soeprapto, Muka Kuning, Batam, Kepulauan Riau.
Kode Pos 29452
Telp : + 6285775710743
E-mail :pb210210088@upbatam.ac.id[1)], andimaslan@puterabatam.ac.id[2)]

Abstract

The advancement of information and communication technology has significantly increased the use of wireless networks (Wifi) due to their flexibility and efficiency. Households, offices, and public institutions widely adopt Wifi. However, this convenience comes with high vulnerability to security threats such as sniffing, spoofing, brute force attacks, and man-in-the-middle attacks. These threats are often exacerbated by weak network configurations and low user awareness. This study aims to implement the Aircrack-ng tool to analyse Wifi security and evaluate its effectiveness in identifying vulnerabilities. The testing method involves stages of scanning, capturing, deauthentication, and cracking, conducted using Kali linux. The research was applied to a Wifi network in the PT Evergrown technology environment. The results show that Aircrack-ng effectively identifies weaknesses, especially in poorly encrypted networks and weak passwords. Handshake data collected via deauthentication was successfully used in the password cracking process. These outcomes demonstrate that Wifi networks remain at risk without proper security settings. As mitigation, the use of strong passwords, disabling WPS, regularly updating firmware, and applying Mac filtering are recommended. Aircrack-ng thus proves useful not only for penetration testing but also as a reference to improve wireless network security.

Keywords: aircrack-ng, kali linux, mac filtering, network security, penetration testing.

Abstrak

Kemajuan teknologi informasi dan komunikasi telah mendorong peningkatan penggunaan jaringan nirkabel (*Wifi*) karena fleksibilitas dan efisiensinya. *Wifi* banyak digunakan di rumah, kantor, dan institusi publik. Namun, kemudahan ini juga membawa kerentanan tinggi terhadap ancaman keamanan seperti sniffing, spoofing, *brute* force, dan man-in-the-middle. Ancaman ini diperparah oleh konfigurasi jaringan yang lemah dan rendahnya kesadaran pengguna. Penelitian ini bertujuan mengimplementasikan *tool Aircrack-ng* untuk menganalisis keamanan *Wifi* serta mengevaluasi efektivitasnya dalam mengidentifikasi celah keamanan. Pengujian dilakukan melalui tahapan scanning, capturing, *deauthentication*, dan *cracking* menggunakan *Kali linux*. Penelitian diterapkan pada jaringan *Wifi* di lingkungan PT *Evergrown technology*. Hasil menunjukkan bahwa *Aircrack-ng* efektif dalam mengidentifikasi kelemahan, terutama pada jaringan dengan enkripsi lemah dan kata sandi yang mudah ditebak. Data *handshake* yang diperoleh melalui serangan *deauthentication* berhasil digunakan dalam proses *cracking*. Temuan ini membuktikan bahwa jaringan *Wifi* tetap rentan tanpa pengaturan keamanan yang memadai. Sebagai upaya mitigasi, disarankan penggunaan kata sandi kuat, menonaktifkan WPS, memperbarui firmware secara berkala, dan menerapkan *Mac filtering*. *Aircrack-ng* terbukti berguna dalam pengujian penetrasi dan sebagai acuan peningkatan keamanan jaringan nirkabel.

Kata kunci: *aircrack-ng*, *kali linux*, keamanan jaringan, *mac filtering*, *penetration testing*

1. Pendahuluan

Jaringan nirkabel (*Wifi*) telah menjadi solusi utama dalam penyediaan layanan konektivitas karena sifatnya yang fleksibel dan efisien. *Wifi* digunakan secara luas di lingkungan rumah, institusi pendidikan, perkantoran, hingga fasilitas umum. Namun demikian, di balik kemudahan tersebut, jaringan *Wifi* memiliki potensi kerentanan yang cukup tinggi terhadap berbagai bentuk ancaman keamanan[1] Ancaman-ancaman tersebut dapat menyebabkan kebocoran informasi, pencurian data, bahkan pengambilalihan akses terhadap sistem.

Kurangnya kesadaran pengguna dan lemahnya konfigurasi keamanan jaringan menjadi salah satu faktor utama yang menyebabkan tingginya tingkat kerentanan tersebut Sifat jaringan nirkabel yang terbuka memungkinkan pihak tidak bertanggung jawab untuk melakukan berbagai jenis serangan, seperti *sniffing, spoofing, brute force attack*, maupun *man-In-the-middle attack*.[2]

Oleh karena itu, diperlukan upaya untuk melakukan analisis terhadap keamanan jaringan *Wifi* guna mengidentifikasi potensi celah keamanan yang ada. Berbagai perangkat lunak *open source* telah tersedia untuk membantu proses pengujian keamanan jaringan, di antaranya Wireshark, Reaver, Wifite, hingga Aircrack-ng.[3] Dari berbagai pilihan tersebut, Aircrack-ng banyak digunakan karena memiliki fokus pada audit keamanan jaringan nirkabel, khususnya dalam menganalisis kelemahan pada sistem enkripsi WEP dan WPA/WPA2. Selain itu, Aircrack-ng terbukti andal dan relatif aman digunakan dalam konteks penelitian maupun *penetration testing* karena bersifat legal, *open source*, serta terus diperbarui oleh komunitas keamanan siber untuk menyesuaikan dengan perkembangan standar enkripsi terbaru.

Dalam implementasinya, *Aircrack-ng* dapat dijalankan secara optimal menggunakan sistem operasi *Kali linux*, yang dikenal sebagai distribusi *Linux* yang ditujukan untuk keperluan *penetration testing[4]* dan keamanan sistem informasi. Melalui kombinasi antara *Aircrack-ng* dan *Kali linux*, dimungkinkan untuk melakukan simulasi serangan terhadap jaringan *Wifi* secara terstruktur dan bertanggung jawab, dengan tujuan utama untuk memperoleh pemahaman yang lebih mendalam mengenai aspek-aspek keamanan jaringan nirkabel.

2. Tinjauan Pustaka

2.1 Jaringan Komputer

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[5][6]

2.2 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.[7] 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.[8] Oleh karena itu, pemahaman menyeluruh mengenai keamanan jaringan sangat diperlukan dengan mempelajari konsep, metode, serta teknologi utama yang digunakan dalam bidang ini[9]

2.3 *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[10]

Berikut teknik-teknik serangan yang umum digunakan.

1. *Bruteforce Attack*, Merupakan serangan yang menebak kombinasi kredensial, seperti *username* dan *password*, berulang kali hingga menemukan kombinasi yang tepat.[11]
2. *Dictionary attack*, merupakan teknik menebak kata sandi di mana penyerang berusaha mengetahui kata sandi pengguna dengan mencoba secara berurutan kata-kata dari sebuah kamus (daftar kata sandi yang dianggap mungkin digunakan). Kamus milik penyerang biasanya tidak terbatas pada kata-kata dari kamus bahasa alami tradisional, tetapi juga dapat mencakup variasi dari nama depan atau belakang pengguna, inisial, nama akun, kata-kata dari berbagai basis data, variasi ejaan dan permutasi, serta pasangan kata yang umum.[12]
3. *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[13]*

2.4 Analisa Penelitian Terdahulu

Keamanan jaringan nirkabel telah menjadi topik penting dalam penelitian karena sifatnya yang terbuka dan rawan terhadap serangan. Menurut Stallings[14], kelemahan utama Wi-Fi terletak pada konfigurasi yang tidak optimal serta penggunaan metode enkripsi yang sudah usang, seperti WEP, yang rentan terhadap serangan *brute force* maupun *dictionary attack*. Penelitian-penelitian sebelumnya banyak berfokus pada analisis kerentanan sistem enkripsi WPA/WPA2 dengan memanfaatkan berbagai tools *penetration testing*.

Penelitian oleh Kolev & Shterev [15] yang berjudul *"Wireless Security Issues"* membahas isu keamanan jaringan nirkabel menggunakan *tools* seperti Airmon-ng dan Aircrack-ng untuk menganalisis lalu lintas jaringan serta mengidentifikasi celah keamanan. Hasil penelitian menunjukkan bahwa deteksi dini terhadap ancaman dapat dilakukan apabila konfigurasi jaringan diperiksa secara berkala.

Penelitian lain yang dilakukan oleh Rahman [16] menekankan efektivitas Aircrack-ng dalam melakukan serangan *dictionary attack* pada jaringan WPA2. Hasilnya menunjukkan bahwa kekuatan kata sandi menjadi faktor paling menentukan dalam keberhasilan serangan. Hal ini menegaskan pentingnya penerapan kebijakan kata sandi yang kuat dan kompleks untuk meminimalisasi risiko kebocoran data.

Sementara itu, studi yang dilakukan oleh Prasetyo [17]menggunakan pendekatan *penetration testing* berbasis Wireshark dan Reaver untuk menguji kelemahan jaringan Wi-Fi pada institusi pendidikan. Penelitian tersebut menemukan bahwa fitur WPS (Wi-Fi Protected Setup) menjadi salah satu titik lemah yang dapat dieksploitasi jika tidak dinonaktifkan.

Berdasarkan penelitian-penelitian terdahulu, dapat disimpulkan bahwa penggunaan tools *penetration testing* seperti Aircrack-ng, Wireshark, maupun Reaver terbukti efektif dalam mengidentifikasi kerentanan jaringan nirkabel. Namun, sebagian besar penelitian hanya berfokus pada uji coba tertentu, seperti serangan *dictionary attack* atau eksploitasi WPS. Dengan demikian, penelitian ini berupaya memberikan kontribusi melalui analisis keamanan jaringan Wi-Fi di lingkungan PT Evergrown Technology dengan pendekatan praktis menggunakan Aircrack-ng pada sistem operasi Kali Linux, untuk memberikan gambaran menyeluruh mengenai tingkat kerentanan serta langkah mitigasi yang dapat diterapkan.

2.5 Tools

Dalam menganalisis dan menguji keamanan jaringan nirkabel, dibutuhkan serangkaian *tools* yang dirancang khusus untuk melakukan pemindaian, eksploitasi, dan pemantauan lalu lintas jaringan. Berikut *tools* yang diguunakan beserta penjelasannya.

1. *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.[18]

2. Packet *tools Aircrack-ng*

merupakan suite perangkat lunak (*tools*et) yang bersifat *open-source* yang dirancang khusus untuk mengaudit keamanan jaringan nirkabel (*Wi-fi*). Fungsi utamanya berfokus pada pemantauan, penyerangan, pengujian, dan peretasan jaringan nirkabel, menjadikannya alat yang tak tergantikan untuk menilai seberapa aman sebuah jaringan *Wi-fi*. 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*.[19]

A. ***Airmon-ng***

Airmon-ng merupakan tools untuk mengaktifkan mode *monitor* (*monitor mode*) pada *wireless network interface card* (kartu jaringan nirkabel). Dalam *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

.

B. ***Airodump-ng***

Airodump-ng merupakan 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.

C. ***Aireplay-ng***

Aireplay-ng merupakan *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*.

D. ***Aircrack***-ng

Aircrack-ng merupakan *tool* untuk memecahkan kata sandi jaringan. Untuk enkripsi *WEP*, *Aircrack-ng* menggunakan serangan statistik berdasarkan IVs yang dikumpulkan. Setelah paket data yang relevan (terutama handshake *WPA/WPA2* atau IVs *WEP*) berhasil ditangkap oleh *Airodump-ng*.

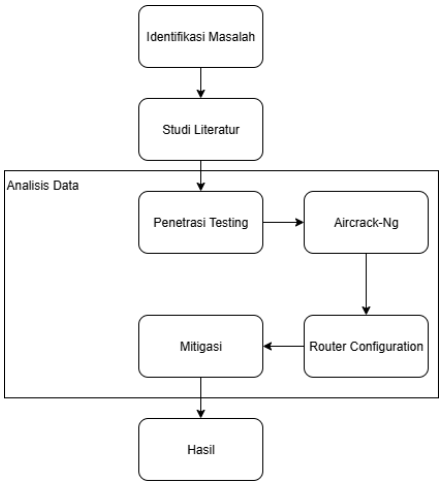
3. *Wireshark*,

Wireshark adalah 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 real-time maupun melalui file hasil tangkapan sebelumnya.[20]

3. Metodologi Penelitian

3.1 Desain Penelitian

Berikut ini merupakan desain penelitian tentang implementasi *tools aircrack-ng* untuk menganalisis keamanan jaringan *wifi*.



Gambar 1 Desain Penelitian

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.

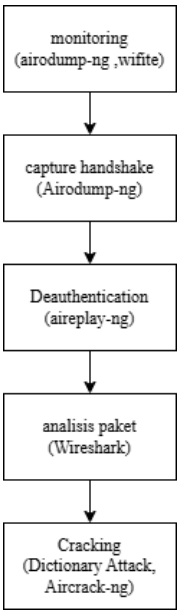
Akhir dari seluruh proses ini menghasilkan hasil penelitian yang mencakup evaluasi efektivitas metode yang diterapkan, kesimpulan atas temuan yang diperoleh, serta rekomendasi untuk peningkatan keamanan jaringan.

3.2 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah metode penetrasi 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 2 Penetrasi Testing

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* 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 Attack*

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.

4. Hasil dan Pembahasan

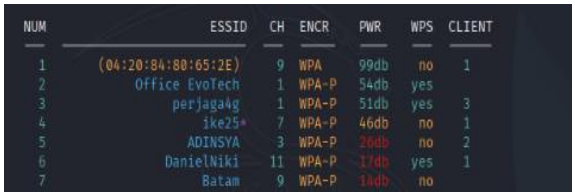
Hasil yang ditampilkan merupakan bukti dari proses implementasi alat dan teknik yang digunakan dalam menganalisis keamanan jaringan *Wifi*, khususnya melalui pemanfaatan *tools Aircrack-ng* pada sistem operasi *Kali linux*. Data yang diperoleh kemudian digunakan sebagai dasar dalam proses analisis serta pembahasan lebih lanjut pada subbab berikutnya

4.1 Hasil Penetrasi Testing

Berikut hasil dari implementasi penetrasi testing menggunakan *aircrack ng* untuk menganalisis keamanan *wifi* di PT *Evergrown technology*, Adapun hasil penetrasi dijelaskan berikut ini:

1. *Monitoring*

Melakukan *Monitoring* menggunakan *Wifite* dan *Airodump-ng* untuk menangkap seluruh jaringan nirkabel yang ada di area sekitar

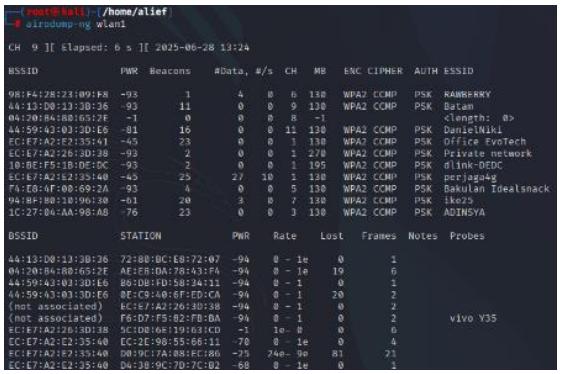


NUM	ESSID	CH	ENCR	PWR	WPS	CLIENT
1	(04:20:84:80:65:2E)	9	WPA	99db	no	1
2	Office EvoTech	1	WPA-P	54db	yes	
3	perjaga4g	1	WPA-P	51db	yes	3
4	ike25*	7	WPA-P	46db	no	1
5	ADINSYA	3	WPA-P	26db	no	2
6	DanielNiki	11	WPA-P	17db	yes	1
7	Batam	9	WPA-P	14db	no	

Gambar 3 *Wifi*te

Pada Gambar 3 di atas menunjukkan hasil pemindaian jaringan nirkabel menggunakan *tool Wifite*. Terlihat bahwa sistem berhasil mendeteksi beberapa jaringan *Wifi* yang berada di sekitar perangkat, lengkap dengan informasi penting seperti nama *SSID (Service Set Identifier*), kekuatan sinyal (*PWR*), jenis enkripsi (*ENCR*), status *WPS*, serta jumlah klien yang terhubung. Salah satu jaringan dengan nama *Office EvoTech* terdeteksi menggunakan enkripsi *WPA-P* dengan kekuatan sinyal sebesar 99 dB dan mengaktifkan fitur *WPS*.

Sementara itu, jaringan seperti *perjaga4g* dan *Ike25* teridentifikasi memiliki fitur WPS aktif, yang mengindikasikan potensi kerentanan terhadap serangan *bruteforce*. Adanya kolom *client* juga menunjukkan jumlah perangkat yang sedang terkoneksi ke masing-masing *access point*, yang dapat dimanfaatkan dalam strategi *deauthentication* atau pengambilan *handshake*. Data ini menjadi dasar awal dalam proses analisis dan pengujian kerentanan pada jaringan *Wifi* yang ditargetkan.

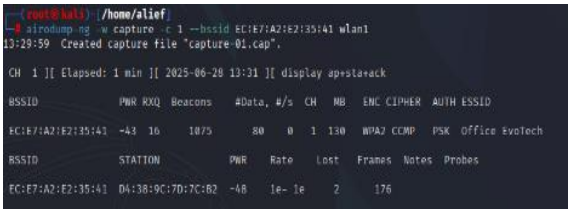


Gambar 4 *Monitoring* dengan *airodump-ng*

Lalu pada Gambar 4 di atas menunjukkan hasil pemindaian jaringan nirkabel menggunakan *tool Airodump-ng* yang dijalankan menggunakan *interface wlan1* dalam mode *monitor.*

Dalam hasil tersebut, SSID *Office EvoTech* dipilih sebagai target utama dalam proses penetrasi jaringan. Jaringan ini memiliki *BSSID* EC:17:2A:25:1C:DC, menggunakan enkripsi *WPA2* dengan *cipher CCMP* dan autentikasi *PSK*, serta berada pada *channel* 1 dengan kekuatan sinyal sebesar -45 dB, yang menunjukkan kualitas sinyal yang cukup baik untuk dilakukan proses intersepsi. Jumlah *beacon* dan lalu lintas data yang terekam juga menunjukkan bahwa jaringan ini aktif dan digunakan oleh klien.

2. *Capture Handshake*

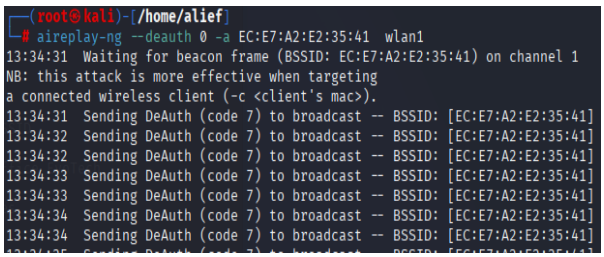


Gambar 5 *Capture Handshake*

Pada proses *capture handshake*, proses ini menggunakan alat bantu *Airodump-ng* untuk menangkap paket autentikasi antara perangkat klien dan *Access point*. Proses ini dilakukan dengan memantau lalu lintas jaringan pada saat perangkat mencoba terhubung ke jaringan *Wi-fi Office EvoTech*.

3. *Deauthentication*

Dilakukan teknik deautentikasi untuk memaksa perangkat klien terputus sementara, sehingga proses *handshake* dapat ditangkap saat perangkat mencoba tersambung Kembali.



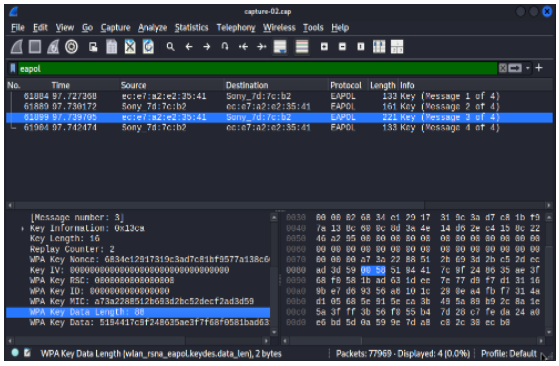
Gambar 6 Proses *Deauthentication*

Ketika perangkat klien mencoba untuk terhubung kembali ke jaringan *Wi-fi* tersebut, proses *handshake* akan berlangsung, dan pada saat itulah paket *handshake* dapat ditangkap, seperti yang ditunjukan pada gambar 7

Gambar 7 *capture Handshake*

4. Analisis paket *handshake*

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

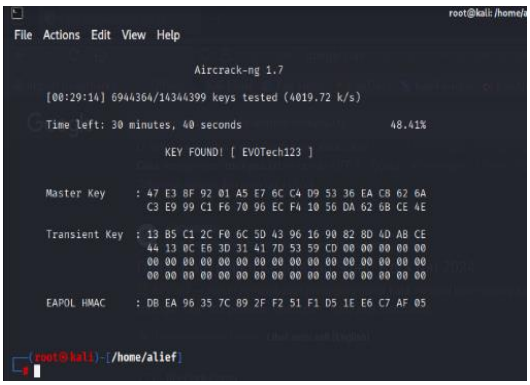


Gambar 8 Analisis Paket *Handshake*

Gambar 8 menunjukkan hasil analisis proses *capture handshake* menggunakan *Wireshark*. Terlihat bahwa proses *4-way handshake* berhasil ditangkap secara lengkap, ditandai dengan adanya empat paket *EAPOL* (*Extensible Authentication Protocol over LAN*) yang masing-masing merepresentasikan *Message* 1 hingga *Message* 4. Dalam detail paket yang ditampilkan, terlihat informasi penting seperti *WPA Key Nonce, WPA Key MIC, dan Key Data* yang merupakan bagian dari proses autentikasi antara perangkat klien dan *Access point*. Data ini menandakan bahwa *handshake* telah terekam dengan baik

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.



Gambar 9 Hasil *Cracking*

Berdasarkan Gambar 9 pengujian menggunakan metode *penetration testing* menunjukkan bahwa jaringan *Wifi* dengan nama *SSID* yang diuji berhasil diretas menggunakan teknik *dictionary attack*. Berdasarkan *output* dari *Aircrack-ng* yang ditampilkan pada Gambar 9 proses dekripsi terhadap file *handshake* berhasil menemukan kata sandi jaringan, yaitu;

$$KEY\ FOUND!\ [EVOTech123]$$

Proses *cracking* ini dilakukan dengan mencocokkan hasil *handshake* yang telah ditangkap sebelumnya dengan daftar kata sandi (*wordlist*) yang tersedia dalam sistem *Kali linux*, dalam hal ini menggunakan file *rockyou.txt*. Hasil pengujian menunjukkan bahwa proses berlangsung dengan kecepatan sekitar 4019.72 k/s, dan berhasil menemukan kunci autentikasi setelah menguji lebih dari 6,9 juta kombinasi dari total sekitar 14,3 juta entri. *Password* berhasil dipecahkan sebelum proses mencapai 50% dari keseluruhan *wordlist*.
Keberhasilan *cracking* ini menunjukkan bahwa:

1. Kata sandi *EVOTech123* tergolong lemah karena masih dapat ditemukan dalam *wordlist*

2. Jaringan *Wi-fi* target tidak cukup kuat dalam hal kebijakan pemilihan kata sandi, karena tidak menggunakan kombinasi kompleks (misalnya karakter khusus, panjang lebih dari 12 karakter, atau penggunaan frasa acak).

3. SSID *Office Evotech* teridentifikasi memiliki fitur WPS aktif, yang mengindikasikan potensi kerentanan terhadap serangan *bruteforce* atau *dictionary attack.*

Serangan *dictionary attack* masih sangat relevan digunakan dalam mengevaluasi keamanan jaringan *Wifi,* khususnya bagi jaringan yang menggunakan kata sandi yang mudah ditebak atau umum digunakan

4.2 Hasil Mitigasi

Berdasarkan hasil pengujian ini, maka langkah-langkah mitigasi yang telah dijabarkan pada Bab 3 menjadi sangat penting untuk diterapkan. Adapun implementasi mitigasi yang dilakukan pada penelitian ini sebagai berikut :

Langkah pertama yaitu *Login* ke Web *Router* melalui *ip address* “192.168.1.1”, dengan menggunakan akun *user*.

Gambar 10 Halaman Login Web *Router*

Berikut data untuk login ke akun *user*:

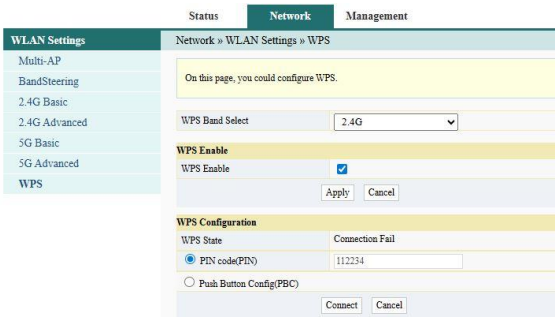
Username : user
Password : user1234

Untuk masuk ke halaman admin menggunakan akun berikut :

Username : Admin
Password : admin

1. Menonaktifkan Fitur *WPS*

Setelah masuk ke konfigurasi *router*, masuk ke halaman *Network*, Klik Menu *WPS*. Maka akan muncul tampilan sebagai berikut.

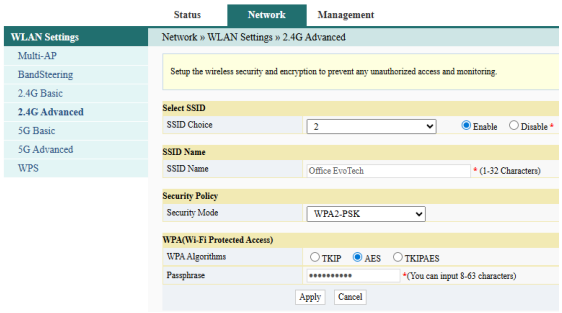


Gambar 11 Menonaktifkan Fitur WPS

Lalu hilangkan centang pada *WPS Enable*, setelah itu Klik *Apply*.

2. Penggunaan Kata Sandi Rumit

Langkah berikutnya yaitu mengganti kata sandi *SSID Office evotech* menggunakan kata sandi yang rumit, setelah sebelumnya dimenu WPS selanjutnya pilih *2,4G Advanced* untuk masuk ke konfigurasi *SSID*, maka akan muncul tampilan sebagai berikut



Gambar 12 Konfigurasi SSID

Lalu isi bagian *passphrase*, sebagai contoh penulis mengisi dengan ”Us3ReV@T3ch”. Setelah selesai klik *apply*.

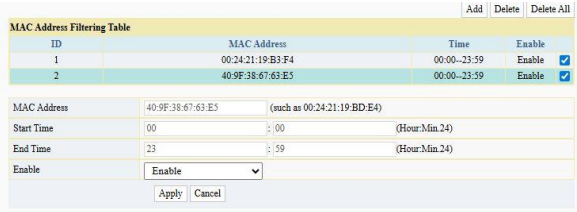
3. Mac filtering

Untuk melakukan *Mac filtering*, masuk ke halaman *web router* menggunakan akun *admin.*

Setelah masuk ke halaman *admin*. Selanjutnya masuk ke menu *security* lalu klik *Mac Filter*, yang berada pada *sub menu firewall*. Seperti pada gambar dibawah ini

Gambar 13 Menu *Mac filtering*

Pilih *enable* pada pilihan *Mac filtering enable*. Lalu pada *Mac filtering Blacklist/Whitelist* pilih *White List*. Yang dimana tujuannya adalah hanya mengijinkan perangkat yang di daftarkan saja yang dapat menggunakan jaringan ini.



Gambar 14 Penerapan *Mac filtering*

Untuk menambahkan *mac address user* klik *add* lalu isi *MAC Address* sesuai dengan pc yang akan di daftarkan. Lalu centang pilihan *enable* pada *checkbox* yang tersedia dalam tabel *mac address*.

4.3 Pembahasan

Pada pembahasan dijelaskan mengenai hasil implementasi dan analisis yang telah dilakukan terhadap keamanan jaringan *Wifi* menggunakan *tools Aircrack-ng*. Adapun pembahasan sebagai berikut.

1. Proses implementasi *tools Aircrack-ng* dalam menganalisis keamanan jaringan *wifi*.

Proses implementasi *tools Aircrack-ng* dalam menganalisis keamanan jaringan *Wifi* diawali dengan *monitoring* menggunakan *tool Airodump-ng* dan *Wifite* untuk melakukan pemindaian jaringan di sekitar dan mengidentifikasi target potensial berdasarkan kekuatan sinyal, jenis enkripsi, serta jumlah klien yang terhubung. Dalam penelitian ini, jaringan *Office EvoTech* dipilih sebagai target utama karena memiliki sinyal kuat dan menerapkan enkripsi WPA2-PSK, yang umum digunakan dalam jaringan kantor. Langkah selanjutnya adalah melakukan serangan *deauthentication* untuk memutus koneksi antara klien dan *access point*, dengan tujuan memicu proses *4-way handshake*. Setelah *handshake* berhasil ditangkap, file hasil tangkapan dianalisis menggunakan *wireshark* untuk memastikan validitas paket *handshake* tersebut. Lalu diproses menggunakan *Aircrack-ng* untuk melakukan serangan *dictionary attack* dengan menggunakan *wordlist* tertentu guna mengidentifikasi password jaringan. Pemilihan *Aircrack-ng* sebagai *tools* utama dalam penelitian ini didasarkan pada beberapa pertimbangan: *tools* ini bersifat *open-source*, memiliki dokumentasi yang luas, serta telah terbukti handal dalam melakukan audit keamanan jaringan nirkabel. Selain itu, *Aircrack-ng* sepenuhnya kompatibel dengan sistem operasi *Kali linux*, dan mendukung berbagai *mode* serangan seperti *WEP cracking*, *WPA/WPA2 handshake capturing*, hingga pengujian kekuatan *password* dengan *wordlist*. Secara keseluruhan, hasil dari proses implementasi menunjukkan bahwa *Aircrack-ng* mampu melakukan pengujian keamanan jaringan *Wifi* dengan efektif. *Handshake* berhasil ditangkap dalam waktu yang relatif singkat setelah proses *deauthentication* dilakukan. Proses *dictionary attack* untuk mengungkap *password* jaringan memerlukan waktu sekitar setengah jam. Waktu ini masih tergolong efisien mengingat pendekatannya yang bersifat *trial and error*. Hasil ini membuktikan bahwa *Aircrack-ng* dapat menjadi alat yang sangat berguna dalam audit keamanan jaringan, khususnya dalam mengidentifikasi kelemahan pada konfigurasi autentikasi jaringan nirkabel berbasis *WPA2-PSK*.

2. Efektivitas *aircrack-ng* dalam mengidentifikasi celah keamanan pada jaringan *wifi*

Aircrack-ng terbukti efektif dalam mengidentifikasi celah keamanan jaringan *Wifi*, khususnya pada jaringan yang menggunakan metode enkripsi *WPA/WPA2-PSK* dan memiliki konfigurasi keamanan standar. Efektivitas *tool* ini terletak pada kemampuannya untuk menangkap paket *handshake* secara *realtime* dan melakukan proses *cracking* terhadap *password Wifi* menggunakan metode *dictionary attack*. Dalam kasus jaringan *Office EvoTech*, *handshake* berhasil ditangkap dalam waktu cukup singkat setelah serangan *deauthentication* dilakukan, yang menunjukkan efektivitas teknik tersebut apabila terdapat klien aktif. Selanjutnya, proses *brute force* terhadap file *handshake* memperlihatkan bahwa keamanan jaringan sangat bergantung pada kompleksitas kata sandi yang digunakan. Jika password menggunakan kombinasi sederhana, *Aircrack-ng* dapat dengan cepat mengidentifikasinya menggunakan *wordlist* yang sesuai. Hal ini menunjukkan bahwa *Aircrack-ng* merupakan alat yang sangat berguna dalam pengujian penetrasi serta audit keamanan jaringan nirkabel

3. Mitigasi dengan menggunakan setiap fitur pada perangkat *router wifi*

Untuk mengurangi risiko dari serangan yang berhasil diidentifikasi melalui proses analisis menggunakan *Aircrack-ng*, diperlukan penerapan langkah mitigasi berbasis fitur yang tersedia pada perangkat *router Wifi*. Salah satu langkah utama adalah menonaktifkan fitur *WPS (Wi-fi Protected Setup)*, karena fitur ini sering kali menjadi titik lemah yang dimanfaatkan dalam serangan *brute force*. Selain itu, pengguna *router* disarankan untuk mengganti kata sandi *Wifi* secara berkala dengan kombinasi yang kompleks, mencakup huruf besar, huruf kecil, angka, dan simbol. *Router* modern juga menyediakan fitur *MAC address filtering*, yang dapat membatasi perangkat yang diizinkan terhubung ke jaringan, serta pengaturan *firewall internal* yang dapat menambah lapisan perlindungan terhadap akses tidak sah. Disarankan juga untuk selalu memperbarui *firmware router* guna menutup potensi celah keamanan

yang ditemukan oleh *vendor*. Penerapan langkah-langkah mitigasi ini secara optimal akan meningkatkan ketahanan jaringan terhadap berbagai bentuk ancaman, serta melengkapi hasil evaluasi yang telah dilakukan melalui pengujian menggunakan *Aircrack-ng.*

5. Kesimpulan

5.1 Simpulan

Penelitian ini membuktikan bahwa metode *penetration testing* efektif dalam mengidentifikasi celah keamanan pada jaringan Wi-Fi di lingkungan PT *Evergrown Technology*. Dengan menggunakan *tools* seperti *Wifite*, *Airodump-ng*, *Wireshark*, dan *Aircrack-ng*, proses pengujian menunjukkan bahwa jaringan masih rentan terhadap serangan, khususnya saat terdapat klien yang aktif. Analisis lebih lanjut melalui *Wireshark* memvalidasi bahwa paket *handshake* yang ditangkap dapat digunakan untuk proses dekripsi. Selain itu, keberhasilan teknik *dictionary attack* menggunakan wordlist *rockyou.txt* menegaskan lemahnya kata sandi yang digunakan. Secara keseluruhan, penelitian ini berhasil mencapai tujuannya dan memberikan kontribusi signifikan dalam bidang keamanan jaringan nirkabel, serta memberikan rekomendasi mitigasi yang dapat diterapkan untuk meningkatkan perlindungan terhadap serangan siber.

5.2 Saran

Berdasarkan hasil penelitian, disarankan agar administrator jaringan menonaktifkan fitur *WPS* karena dapat menjadi celah keamanan. Penggunaan kata sandi yang kompleks juga penting untuk mencegah serangan, dengan menghindari kata-kata umum yang mudah ditebak. Selain itu, penerapan *MAC filtering* dapat membatasi akses hanya pada perangkat tertentu. Untuk penelitian selanjutnya, sebaiknya cakupan diperluas ke jaringan dengan konfigurasi keamanan berbeda serta menguji efektivitas mitigasi seperti *WPA3*, *captive portal*, dan segmentasi jaringan.

Ucapan Terima kasih

Penulis mengucapkan terima kasih kepada PT *Evergrown Technology* yang telah memberikan izin dan kesempatan untuk melakukan penelitian di lingkungan Perusahaan, sehingga penelitian ini dapat terlaksana dengan baik. Dan penulis juga menyampaikan apresiasi dan rasa hormat yang setinggi-tingginya kepada Universitas Putera Batam.

Daftar Rujukan

[1] A. Okario *et al.*, "Analisis Celah Keamanan Jaringan WPA dan WPA2 Dengan Menggunakan Metode Penetration Testing," Aug. 2023.

[2] F. Setyawan and H. Amnur, "Keamanan Jaringan Wireless Dengan Kali Linux," 2022. [Online]. Available: http://jurnal-itsi.org

[3] M. A. Adiguna and B. W. Widagdo, "Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r)," 2022.

[4] F. Anam and F. Fachri, "EVALUASI KERENTANAN KEAMANAN JARINGAN NIRKABEL MENGGUNAKAN METODE PENETRATION TESTING DENGAN AIRCRACK-NG," *Rabit : Jurnal Teknologi dan Sistem Informasi Univrab*, vol. 10, no. 1, pp. 1–8, Jan. 2025, doi: 10.36341/rabit.v10i1.5387.

[5] A. EKKLESIA TANGKOWIT, verry ronny palilingan, and olivia eunike selvie liando, "ANALISIS DAN PERANCANGAN JARINGAN KOMPUTER DI SEKOLAH MENENGAH PERTAMA," *EduTIK : Jurnal Pendidikan teknologi informasi dan komunikasi*, vol. 1, Feb. 2021.

[6] S. Sitohang, "MONITORING JARINGAN MIKROTIK MENGGUNAKAN THE DUDE DAN BOT TELEGRAM," *JURNAL COMASIE*, vol. 10, no. 2, 2024.

[7] K. Kolev and Y. Shterev, "Wireless security issues," in *Vide. Tehnologija. Resursi - Environment, Technology, Resources*, Rezekne Higher Education Institution, 2024, pp. 150–154. doi: 10.17770/etr2024vol4.8186.

[8] B. Issac, R. Chiong, and S. M. Jacob, "Analysis of Phishing Attacks and Countermeasures." [Online]. Available: https://logon.rhbbank.com

[9] R. Pratama and J. A. Yani No, "Literature Review : Network Security Menggunakan Virtual Private Network L2TP/IPSEC, Port Knocking, Port Forwarding, Honeypot Dan Pfsense," *Jurnal Jaringan Komputer dan Keamanan JJKK*, vol. 04, no. 03, pp. 11–18, 2023.

[10] M. I. Susanto, A. Hasad, and M. Amin Bakri, "Sistem Proteksi Jaringan Wlan Terhadap Serangan Wireless Hacking," *JREC Journal of Electrical and Electronics*, vol. 7, no. 1, 2019.

[11] D. Hidayat and R. Ramli, "Mengoptimalkan Pencegahan Serangan Brute Force pada Linux melalui Penerapan Metode Aplikasi IDS Snort," *JiTEKH*, vol. 11, no. 2, pp. 57–61, Aug. 2023, doi: 10.35447/jitekh.v11i2.764.

[12] C. Adams, "Dictionary Attack," in *Encyclopedia of Cryptography, Security and Privacy*, S. Jajodia, P. Samarati, and M. Yung, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2019, pp. 1–2. doi: 10.1007/978-3-642-27739-9_74-2.

[13] S. Jain, S. Pruthi, V. Yadav, and K. Sharma, "Penetration Testing of Wireless EncryptionProtocols," in *2022 6th International Conference on Computing Methodologies and Communication (ICCMC)*, 2022, pp. 258–266. doi: 10.1109/ICCMC53470.2022.9754042.

[14] W. Stallings, *Cryptography and Network Security: Principles and Practice*. London: Pearson, 2021. [Online]. Available: https://www.pearson.com/en-us/subject-catalog/p/cryptography-and-network-security-principles-and-practice/P200000007614/9780134444284

[15] K. Kolev and Y. Shterev, "Wireless Security Issues," *Engineering for Rural Development*, vol. 23, 2024, [Online]. Available: https://journals.rta.lv/index.php/ETR/article/view/8186

[16] A. Rahman, "Analisis Serangan Dictionary Attack pada WPA2 Menggunakan Aircrack-ng," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 9, no. 2, pp. 150–157, 2022, [Online]. Available: https://jtiik.ub.ac.id/index.php/jtiik/article/view/XXXX

[17] H. Prasetyo and et al., "Pengujian Keamanan Wireless Access Point Menggunakan Wireshark dan Reaver," *Jurnal Ilmiah Komputer dan Informatika (KOMPUTA)*, 2021, [Online]. Available: https://garuda.kemdikbud.go.id/documents/detail/2227294

[18] H. J. Lu and Y. Yu, "Research on WiFi Penetration Testing with Kali Linux," *Complexity*, vol. 2021, 2021, doi: 10.1155/2021/5570001.

[19] Muhammad Farhan Fauzan and Agung Susilo Yuda Irawan, "WIRELESS ATTACK : MENGGUNAKAN TOOLS AIRCRACK PADA KALI LINUX UNTUK MELAKUKAN WPA ATTACK," *JURNAL LENTERA*, vol. 20, 2021.

[20] B. Mala, S. Agrawal, A. Sharma, R. Kaur, and B. E. Scholars, "Exploring Wireshark for Network Traffic Analysis," *International Journal for Multidisciplinary Research (IJFMR)*, vol. 5, no. 6, Nov. 2023, [Online]. Available: www.ijfmr.com