LAPORAN KEGIATAN PENELITIAN

"Pengembangan Tool Penetration Testing untuk Akuisisi dan Cracking WPA2 Menggunakan Teknik 4-Way Handshake"

Disusun oleh:

Dhanendra Nivadirrokhman	**(S1 Teknik Komputer)**
Aja Wan Habibie	**(S1 Teknik Komputer)**
Raihan Salman Baehaqi	**(S1 Teknik Komputer)**
Agatha Kinanthi P. T. A.	**(S1 Teknik Komputer)**

SECURITY LABORATORY

UNIVERSITAS TELKOM

BANDUNG

2025

ABSTRAK

Penelitian ini bertujuan untuk mengembangkan sebuah tool penetration testing terintegrasi yang dapat melakukan proses scanning, monitoring, packet injection, dan akuisisi pada jaringan Wi-Fi WPA2 melalui teknik serangan 4-Way Handshake otomatis. Tool ini dikembangkan menggunakan Python dengan antarmuka grafis (GUI) berbasis PyQt, mengintegrasikan tools seperti aircrack-ng, hcxpcaptool, dan hashcat untuk pemindaian jaringan, penangkapan paket handshake, serta cracking password menggunakan dictionary attack, yang mendukung jaringan 2.4 GHz dan 5 GHz. Hasil pengujian menunjukkan tool mampu menangkap dan mendeskripsi hash WPA2 secara efektif, serta memberikan rekomendasi peningkatan keamanan jaringan nirkabel. Penelitian ini diharapkan dapat memberikan kontribusi praktis dalam peningkatan kesadaran dan kemampuan keamanan jaringan nirkabel di Indonesia.

Keywords: penetration testing, WPA2 security, PMKID attack, 4-Way Handshake, GUI, PyQt5, hashcat, keamanan jaringan.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan jaringan nirkabel (Wi-Fi) telah menjadi perhatian utama dalam era digital saat ini. Meskipun protokol WPA2 (Wi-Fi Protected Access 2) dianggap relatif aman, beberapa kerentanan masih ditemukan yang dapat dieksploitasi oleh pihak tidak bertanggung jawab. Pengujian penetrasi (penetration testing) menjadi metode penting untuk mengidentifikasi kelemahan sebelum dapat dimanfaatkan oleh penyerang. Namun, alat-alat pengujian keamanan Wi-Fi yang ada saat ini umumnya terfragmentasi dan memerlukan keahlian khusus untuk mengoperasikannya, membuat proses pengujian menjadi kompleks dan tidak efisien.

1.2 Pandangan Penulis Sebelumnya

Penulis sebelumnya menilai bahwa alat-alat penetration testing untuk jaringan WPA2 umumnya masih terfragmentasi, di mana proses seperti scanning, packet capture, dan dekripsi hash harus dilakukan menggunakan tool terpisah. Selain itu, sebagian besar solusi yang tersedia masih berbentuk script terminal berbasis CLI (Command Line Interface) yang membutuhkan pengetahuan teknis mendalam serta konfigurasi manual yang kompleks.

Kondisi ini dinilai tidak efisien dan menyulitkan bagi pengguna yang ingin melakukan pengujian keamanan secara cepat dan praktis. Oleh karena itu, penulis memandang pentingnya pengembangan sebuah tool terintegrasi dengan antarmuka grafis (UI) yang mampu menyederhanakan alur kerja dan memadukan seluruh fungsi penting dalam satu platform.

1.3 Kondisi dan Potensi Wilayah

Di Indonesia, khususnya di lingkungan kampus dan perkotaan, penggunaan jaringan Wi-Fi sangat luas dan menjadi bagian integral dari infrastruktur komunikasi. Namun, kesadaran dan kemampuan untuk menguji keamanan jaringan masih terbatas. Pengembangan alat pengujian penetrasi yang mudah digunakan akan membantu administrator jaringan dan profesional keamanan lokal untuk melakukan audit keamanan secara rutin dan efisien.

1.4 Manfaat jangka Panjang

Pengembangan tool penetration testing terintegrasi akan memberikan kontribusi jangka panjang dalam meningkatkan keamanan infrastruktur jaringan nirkabel di Indonesia. Alat ini dapat menjadi standar dalam pengujian keamanan Wi-Fi, memungkinkan identifikasi dan mitigasi kerentanan lebih cepat, serta meningkatkan kesadaran tentang pentingnya keamanan jaringan di berbagai sektor.

1.5 Luaran Kegiatan

Luaran dari kegiatan penelitian ini adalah:

- Tool penetration testing all-in-one dengan antarmuka pengguna yang intuitif
- Dokumentasi lengkap tentang penggunaan tool dan interpretasi hasil

1.6 Manfaat Kegiatan

Kegiatan ini memberikan manfaat berupa:

- Peningkatan efisiensi dalam pengujian keamanan jaringan Wi-Fi.
- Kontribusi terhadap peningkatan keamanan infrastruktur nirkabel.
- Penyediaan alat pembelajaran praktis untuk pendidikan di bidang keamanan jaringan.
- Penguatan kemampuan sumber daya manusia lokal dalam melakukan audit keamanan jaringan.

BAB II
TINJAUAN PUSTAKA

2.1 Penestration Testing

Penetration testing atau pengujian penetrasi adalah metodologi pengujian keamanan sistem dengan mensimulasikan serangan dari pihak tidak bertanggung jawab untuk mengidentifikasi kerentanan sebelum dapat dieksploitasi [1]. Engebretson [2] mendefinisikan penetration testing sebagai proses evaluasi keamanan sistem melalui simulasi serangan terhadap sistem untuk mengidentifikasi kelemahan yang dapat berpotensi memungkinkan akses tidak sah.

2.2 Metodologi Penetration Testing

Weidman [3] mengklasifikasikan metodologi penetration testing menjadi beberapa tahap: reconnaissance (pengumpulan informasi), scanning (pemindaian), exploitation (eksploitasi), dan post-exploitation (pasca-eksploitasi). Dalam konteks keamanan Wi-Fi, Ramachandran dan Buchanan [4] menekankan pentingnya fase reconnaissance dan scanning untuk mengidentifikasi jaringan target, sedangkan fase exploitation mencakup akuisisi hash dan cracking password.

Metodologi PTES (Penetration Testing Execution Standard) yang dibahas oleh Herzog et al. [5] menyediakan kerangka kerja terstandarisasi untuk melakukan pengujian penetrasi yang komprehensif, mencakup pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, dan reporting.

2.3 Penetration Testing pada Jaringan Wi-Fi

Dalam konteks jaringan nirkabel, penetration testing memiliki karakteristik unik dibandingkan dengan penetration testing pada jaringan kabel konvensional. Akses yang tidak memerlukan koneksi fisik membuat jaringan Wi-Fi rentan terhadap serangan dari jarak jauh.

Penelitian oleh Bartoli et al. [6] menunjukkan bahwa 78% jaringan Wi-Fi komersial rentan terhadap minimal satu jenis serangan, dengan serangan terhadap WPA2 menjadi yang paling umum. Studi oleh Nur dan Saputra [7] di Indonesia menyimpulkan bahwa 65%

jaringan Wi-Fi di area publik menggunakan passphrase yang lemah, menjadikannya rentan terhadap serangan brute force dan dictionary attack.

2.4 Standar dan Etika Penetration Testing

Pengujian penetrasi harus dilakukan dengan memperhatikan aspek legal dan etika. Mujawar et al. [8] menekankan pentingnya mendapatkan izin tertulis sebelum melakukan pengujian untuk menghindari implikasi hukum. Dalam konteks Indonesia, UU ITE memberikan batasan yang jelas mengenai tindakan yang dapat diklasifikasikan sebagai peretasan ilegal.

Simpson [9] mengidentifikasi beberapa komponen kunci dalam izin pengujian penetrasi, termasuk ruang lingkup, waktu, metode yang disetujui, dan pemberitahuan kepada pihak terkait. Dalam konteks akademis, pengujian penetrasi sering dilakukan dalam lingkungan terkontrol atau pada infrastruktur yang dimiliki oleh peneliti sendiri.

2.5 Protokol Keamanan Wi-Fi

Evolusi protokol keamanan jaringan nirkabel telah berkembang secara signifikan untuk mengatasi berbagai kerentanan yang ditemukan seiring waktu. Tsitroulis et al. [10] memaparkan perkembangan dari protokol Wired Equivalent Privacy (WEP) yang rentan, menuju Wi-Fi Protected Access (WPA), hingga implementasi WPA2 dan WPA3 yang menawarkan tingkat keamanan lebih tinggi. Meskipun WPA2 mengimplementasikan enkripsi Advanced Encryption Standard (AES) yang dianggap kuat, Vanhoef dan Piessens [11] mengungkapkan kerentanan fundamental pada protokol 802.11i yang mendasari WPA2, yang disebut Key Reinstallation Attacks (KRACK), memungkinkan penyerang untuk memanipulasi kunci enkripsi.

Implementasi WPA2 dalam lingkungan enterprise maupun personal memiliki karakteristik keamanan yang berbeda. Celosia dan Cunche [12] mendemonstrasikan bahwa WPA2 Enterprise dengan EAP-TLS secara teoritis menawarkan keamanan yang lebih kuat, namun implementasi yang tidak tepat sering menjadi vektor serangan. Sejalan dengan temuan tersebut, Kohlios dan Hayajneh [13] mengkonfirmasi bahwa mayoritas jaringan Wi-Fi saat ini masih menggunakan WPA2-PSK (Pre-Shared Key) yang bergantung pada passphrase

statis, meningkatkan kerentanannya terhadap serangan offline berupa dictionary attack dan brute force.

2.6 Ancaman Keamanan pada Jaringan Wi-Fi

Kerentanan pada jaringan Wi-Fi telah dikategorikan dalam beberapa kelompok serangan utama. Rahman et al. [14] mengklasifikasikan ancaman keamanan Wi-Fi menjadi beberapa jenis, termasuk man-in-the-middle attacks, rogue access point attacks, dan password cracking. Penelitian oleh Bhanot dan Hans [15] mendokumentasikan bahwa lebih dari 60% jaringan Wi-Fi korporat dan pribadi masih rentan terhadap eksploitasi karena konfigurasi tidak aman dan penggunaan password yang lemah.

Perkembangan teknologi telah meningkatkan efektivitas upaya penetrasi terhadap jaringan WPA2. Baek et al. [16] berhasil mendemonstrasikan bahwa jaringan WPA2-PSK dengan kunci yang lemah dapat dikompromikan dalam waktu kurang dari 24 jam menggunakan teknik dictionary attack yang dioptimalkan. Sejalan dengan temuan ini, Yang et al. [17] menunjukkan bahwa kemajuan komputasi paralel dan teknologi GPU telah secara dramatis meningkatkan efisiensi password cracking, dengan kecepatan modern mencapai miliaran percobaan per detik untuk WPA2-PSK.

2.7 Keamanan Jaringan Nirkabel WPA2

Protokol WPA2 (Wi-Fi Protected Access 2) merupakan standar keamanan jaringan nirkabel yang diperkenalkan pada tahun 2004 sebagai pengganti WPA dan WEP, dengan tujuan mengatasi kelemahan pada protokol sebelumnya [18]. WPA2 menggunakan algoritma enkripsi Advanced Encryption Standard (AES) dan protokol Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) yang menawarkan tingkat keamanan lebih tinggi dibandingkan protokol pendahulunya [19].

Vanhoef dan Piessens [20] mengidentifikasi kerentanan pada WPA2 yang dikenal sebagai KRACK (Key Reinstallation Attacks), yang memungkinkan penyerang untuk mengganggu proses key installation dan potensial mendekripsi komunikasi. Selain itu, studi oleh Sýkora et al. [21] menunjukkan bahwa meskipun WPA2 menawarkan enkripsi yang kuat, kelemahan sering terletak pada penggunaan password yang lemah, memungkinkan serangan berbasis kamus atau brute force berhasil.

Supriyanto [22] dalam penelitiannya di lingkungan kampus Indonesia menemukan bahwa lebih dari 60% jaringan Wi-Fi yang menggunakan WPA2 masih rentan terhadap serangan karena penggunaan passphrase yang mudah ditebak. Temuan ini menegaskan pentingnya pengujian penetrasi sebagai langkah proaktif dalam mengidentifikasi kerentanan.

2.8 Teknik 4-Way Handshake

Teknik 4-Way Handshake merupakan metode klasik dalam pengujian keamanan WPA2 yang memanfaatkan proses autentikasi antara access point dan client [23]. Serangan deauthentication, seperti yang dianalisis oleh Ahmad dan Yaacob [24], dapat memaksa client untuk melakukan proses autentikasi, memungkinkan penangkapan handshake oleh penyerang.

Tian et al. [25] menunjukkan bahwa keberhasilan metode ini bergantung pada keberadaan client aktif yang terkoneksi ke jaringan target, serta kecepatan dalam menangkap paket handshake. Penelitian oleh Putra et al. [26] di Indonesia mengkonfirmasi efektivitas teknik ini pada jaringan dengan traffic tinggi, dengan tingkat keberhasilan mencapai 85% pada penangkapan handshake.

2.9 Teknik PMKID

Teknik PMKID merupakan metode yang lebih baru untuk akuisisi hash WPA2, diperkenalkan pada tahun 2018 oleh Jens "atom" Steube [27]. Keunggulan utama dari teknik ini adalah kemampuannya untuk mendapatkan hash tanpa memerlukan keberadaan client aktif dan tanpa mengirimkan paket deauthentication yang dapat mengganggu konektivitas jaringan [28].

Dibandingkan dengan teknik 4-Way Handshake, metode PMKID memiliki tingkat keberhasilan yang lebih tinggi pada jaringan dengan client terbatas. Namun, penelitian Zhao dan Wang [29] menemukan bahwa tidak semua perangkat access point mendukung atau merespons permintaan PMKID, dengan tingkat dukungan hanya sekitar 70% pada perangkat terbaru.

2.10 Cracking Password

Password cracking merupakan proses mengkonversi hash password kembali ke bentuk plaintext aslinya. Dalam konteks keamanan jaringan, cracking dapat digunakan untuk tujuan forensik digital dan pengujian keamanan sistem [30]. Proses ini menjadi bagian integral dalam penetration testing jaringan WPA2, dilakukan untuk memverifikasi kekuatan password yang digunakan.

2.11 Framework Pengembangan Graphical User Interface

PyQt5 dan Tkinter merupakan framework yang populer untuk pengembangan GUI dalam bahasa pemrograman Python. Namun, penelitian oleh Kurniawan et al. [31] menunjukkan bahwa PyQt5 menawarkan fleksibilitas dan performa yang lebih baik untuk aplikasi yang memerlukan multithreading dan pemrosesan real-time, seperti pada tools monitoring jaringan.

2.12 Literatur Terkait

Pada penelitian terkait "Pengembangan Tool Penetration Testing untuk Akuisisi dan Cracking WPA2 Menggunakan Teknik PMKID dan 4-Way Handshake", studi literatur yang menjadi referensi, yaitu:

- Penelitian oleh Vanhoef (2017) membuktikan kerentanan pada 4-Way Handshake (KRACK).

BAB III
PERANCANGAN & IMPLEMENTASI SISTEM

3.1 Analisis Kebutuhan

3.1.1 Kebutuhan Fungsional

Kebutuhan fungsional dari sistem yang akan dibangun meliputi:

1. Sistem dapat melakukan pemindaian (scanning) jaringan Wi-Fi yang tersedia di sekitar.
2. Sistem dapat mengakuisisi hash WPA2 menggunakan dua metode:
   - 4-Way Handshake (dengan melakukan deauth pada klien aktif).
3. Sistem dapat mengonversi hash ke format yang dapat dibaca oleh alat cracking seperti Hashcat.
4. Sistem dapat melakukan proses cracking password menggunakan wordlist yang telah ditentukan.
5. Sistem menampilkan hasil proses (password ditemukan/tidak, waktu cracking, dan metode yang digunakan).

3.1.2 Kebutuhan Teknis

Untuk menunjang pengembangan dan pengoperasian sistem, dibutuhkan:

1) Perangkat keras:
   - Laptop/PC dengan GPU (NVIDIA) untuk proses cracking cepat.
   - Wireless Adapter yang mendukung Monitor Mode dan Packet Injection (Contoh: Alfa AWUS036NHA).
2) Perangkat lunak:
   - Sistem operasi Linux (Kali Linux).
   - Tools: aircrack-ng, hexdump tool, hcx pcapng tool, hashcat, tcpdump, airodump-ng, aireplay-ng.
   - Wordlist untuk dictionary attack (contoh: rockyou.txt).
3) Koneksi internet untuk pengunduhan tools tambahan dan update library wordlist.

3.2 Penjelasan Sistem

Aplikasi ini dibangun menggunakan Python dengan antarmuka GUI berbasis PyQt5. Fungsionalitas utamanya dibagi ke dalam dua proses besar: Pemindaian jaringan (Scan) dan Penangkapan & cracking (Capture & Crack).

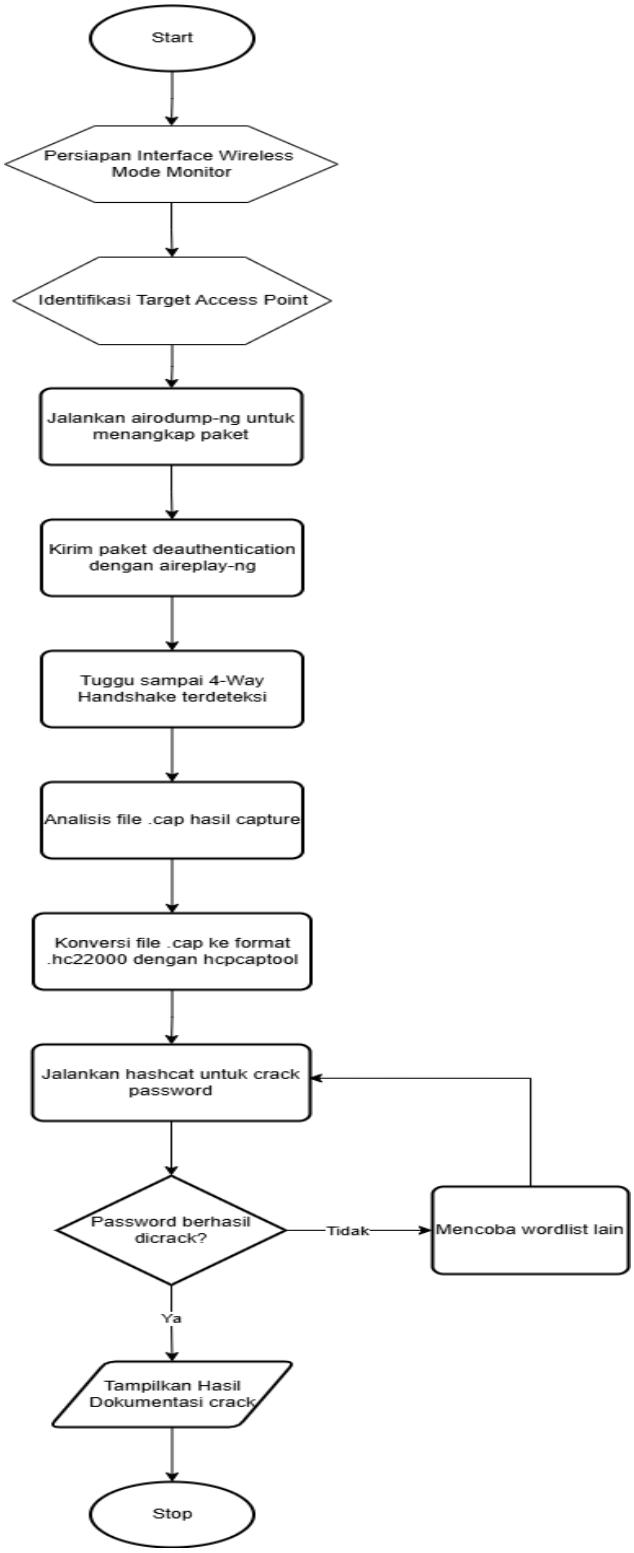
Komponen Utama:

- **ScanThread:** Menyiapkan antarmuka ke mode monitor, menjalankan airodump-ng untuk menemukan jaringan Wi-Fi, lalu menampilkan SSID, BSSID, dan channel.
- **CaptureThread:**
    1) Menjalankan airodump-ng untuk menangkap paket.
    2) Mengirim paket deauth dengan aireplay-ng.
    3) Menganalisis file .cap, mengonversi ke .hc22000 menggunakan hcxpcaptool.
    4) Menjalankan hashcat untuk mencoba melakukan crack password.
- **WiFiCrackerApp:** GUI utama yang menampilkan jaringan, menerima input pengguna, dan menampilkan log serta hasil proses secara real-time.

3.3 Alur Kerja

Langkah-langkah yang dilakukan sistem secara berurutan:

1) Scanning Jaringan: Mengubah interface ke monitor mode lalu melakukan pemindaian dengan airodump-ng.
2) Pemilihan Target: Pengguna memilih jaringan (SSID & BSSID).
3) Penangkapan Handshake: Sistem menangkap menggunakan 4 way handshake
4) Konversi Hash: File .cap dikonversi ke .hc22000.
5) Cracking Password: hashcat melakukan brute-force berdasarkan wordlist.
6) Hasil: Ditampilkan status keberhasilan, waktu eksekusi, dan informasi tambahan.



Gambar 1. Diagram Alur Kerja

3.4 Perangkat

Adapun perangkat yang akan digunakan dalam sistem berikut di antara lain adalah:

No	Nama Barang	Spesifikasi
1	Laptop/PC	Minimal Intel i5, NVIDIA GPU (support CUDA), RAM 8GB+
2	Wireless Adapter	TP-LINK Archer T2U Plus AC600 (Dual Band), modified rtl188eus
3	OS	Kali Linux
4	Software Tools	aircrack-ng, hashcat, hcxpcaptool
5	Python Modules	PyQt5, subprocess, os, threading

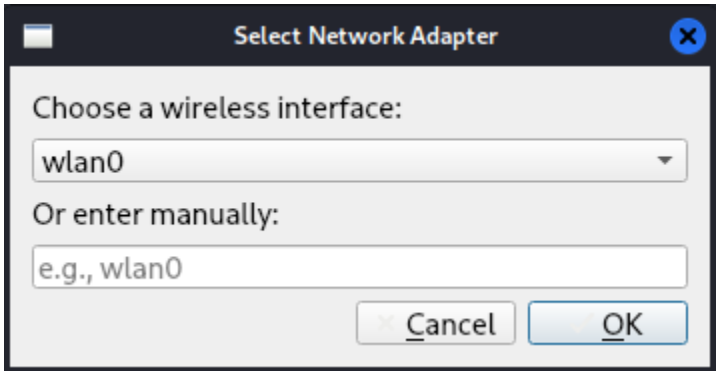
Table 1. Perangkat

BAB IV
HASIL & ANALISIS SISTEM

4.1 Alur Penggunaan Tools

1. Select Network Adapter

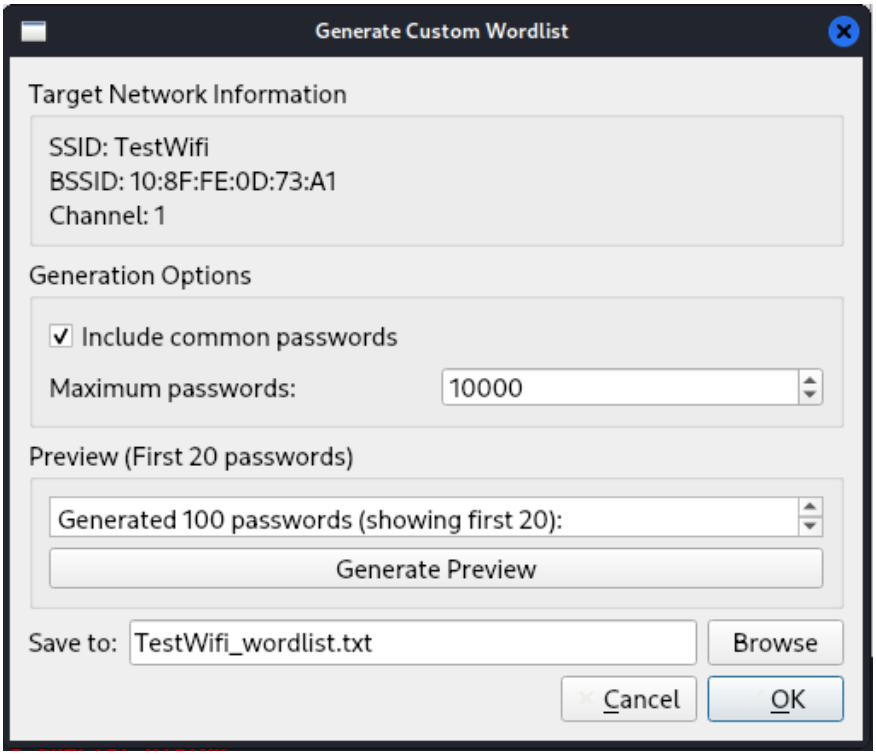
Pada *interface* awal aplikasi, diberikan pilihan *adapter* yang digunakan sebagai *tools* untuk melakukan *wifi cracking*. Misalnya, *wireless adapter* yang digunakan adalah ***wlan0***.



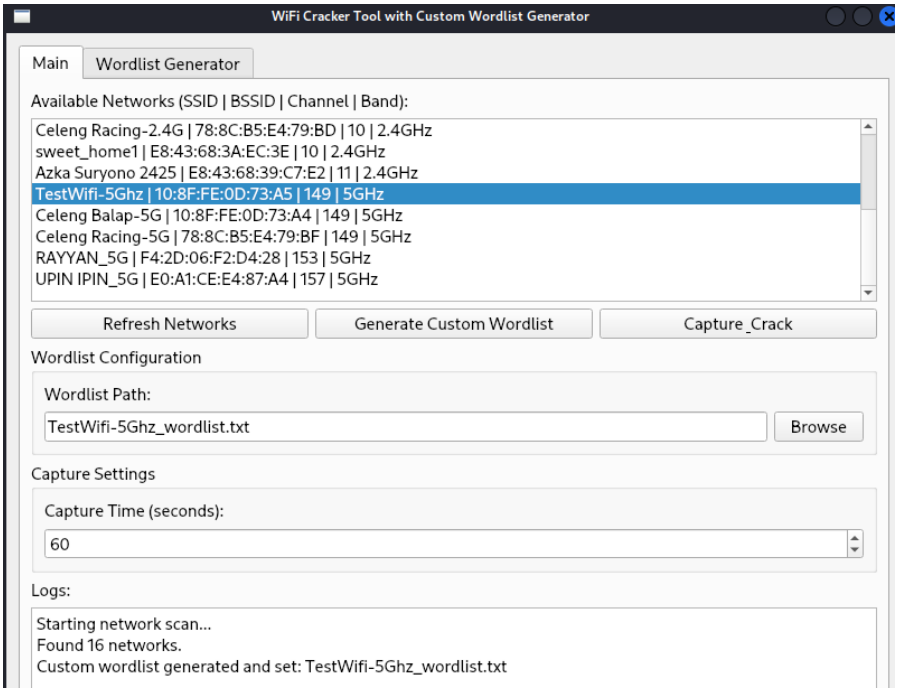
Gambar 2. Opsi Network Adapter

2. Wordlist Generator

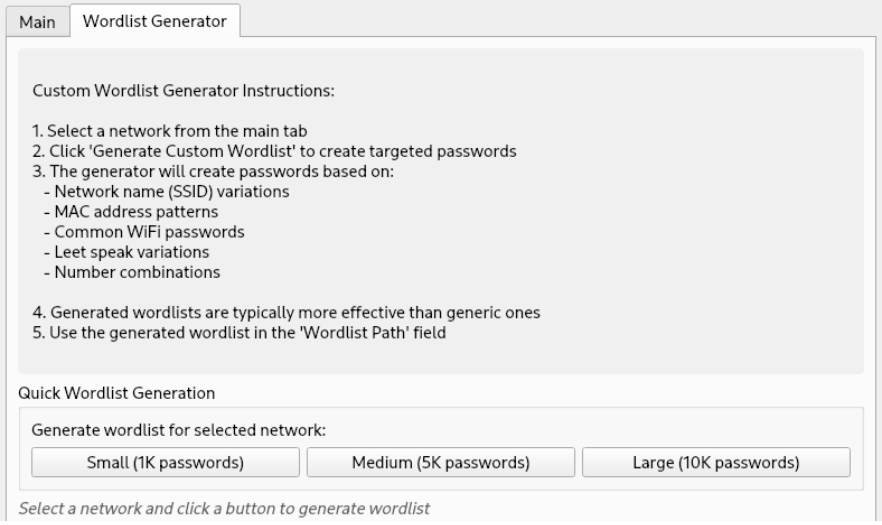
Pada sistem diberikan opsi untuk melakukan generate wordlist. Pada kasus ini dapat di generate sebanyak 10000 password dimana outputnya terdapat pada TestWifi_wordlist.txt. Pada bagian ini, pengguna dapat melakukan pengecekan network yang akan di tes serta wordlist yang akan digunakan nantinya.



Gambar 3. Opsi Wordlist Generator



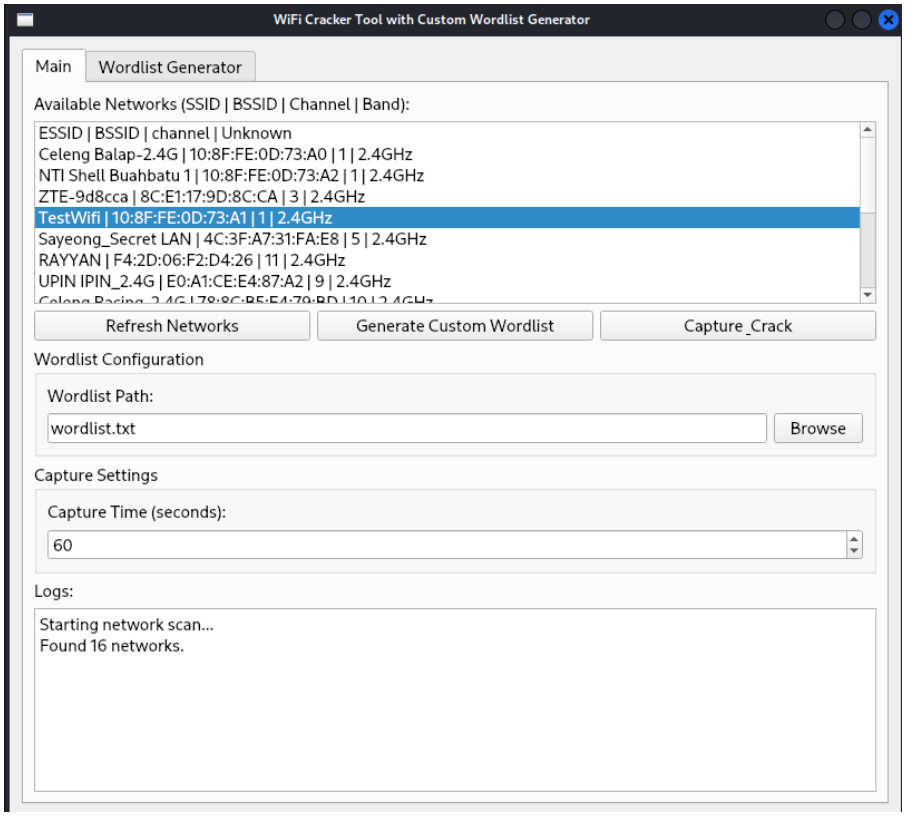
Gambar 4. Pemilihan Network Target



Gambar 5. Opsi wordlist

3. Proses Scanning

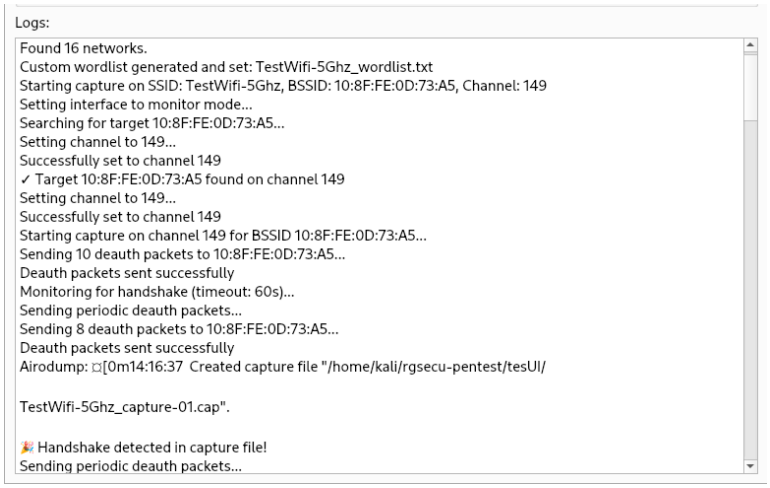
Tampilan utama *tool* setelah *network scan* dilakukan, menampilkan daftar jaringan yang tersedia dan konfigurasi *wordlist* serta pengaturan *capture*.



Gambar 6. Proses Scanning

4. **Proses Capturing EAPOL (menggunakan metode dauthenticate client)**

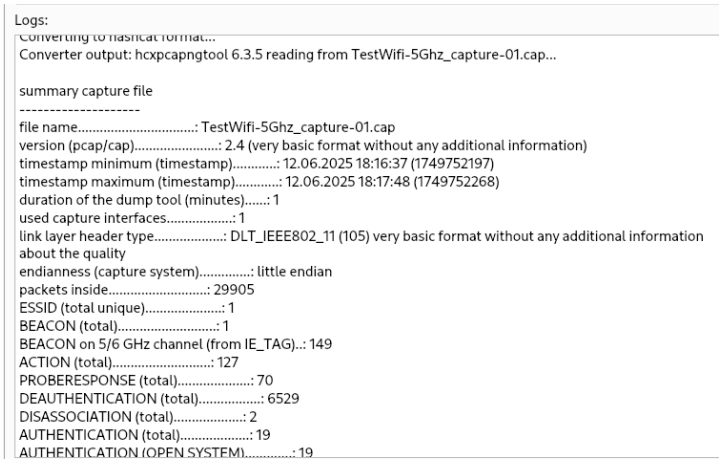
   Proses *capture* dimulai pada SSID target, *interface* diatur ke *monitor mode*, dan *channel* disesuaikan. *Deauthentication packets* dikirim untuk memaksa klien melakukan *re-authentication*, sehingga *handshake* dapat ditangkap.



Gambar 7. Proses Capturing EAPOL

5. **Processing File .cap**

   File .cap yang berhasil ditangkap kemudian di-*convert* ke format yang kompatibel dengan *hashcat* (.hc22000) menggunakan hcxpcaptool. Ringkasan *capture file* juga ditampilkan, termasuk jumlah paket yang ditangkap dan detail jaringan.



Gambar 8. Proses Capture File .cap

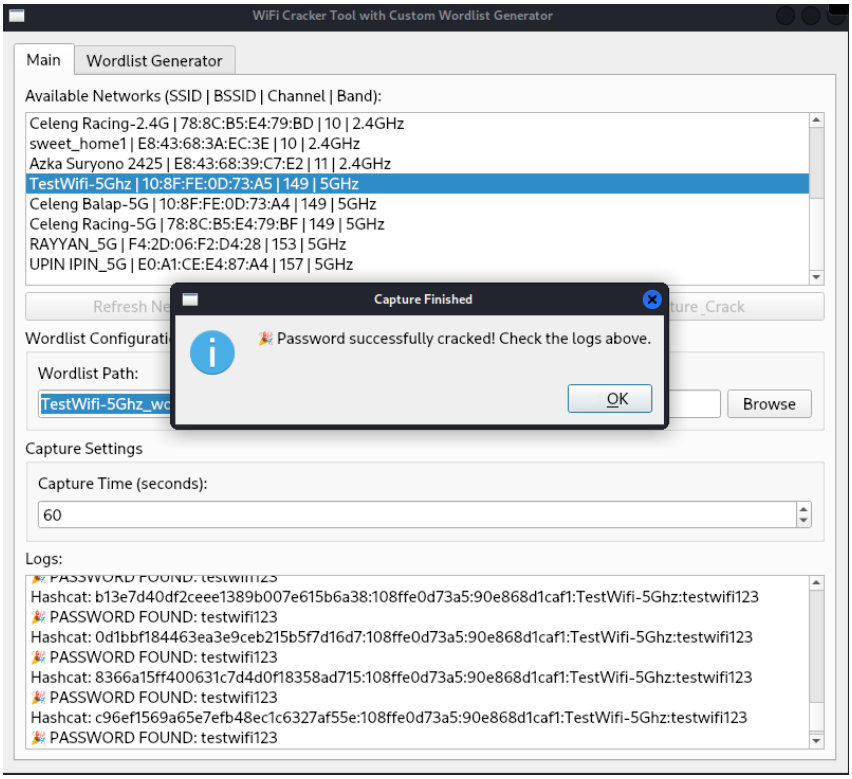
6. **Dictionary Attack menggunakan hashcat**

Setelah *file hash* siap, hashcat dijalankan dengan *wordlist* yang telah disiapkan untuk melakukan *dictionary attack*. Proses ini mencoba mencocokkan *hash* dengan *password* yang ada di *wordlist*.

Gambar 9. Dictionary Attack

7. **Password Berhasil di Crack Menggunakan Custom Dictionary**

   Jika *password* ditemukan dalam *wordlist*, *tool* akan menampilkan *password* yang berhasil di-*crack* beserta *hash*nya. Sebuah notifikasi juga akan muncul menandakan proses *cracking* selesai dan berhasil.



Gambar 10. Password Crack

4.2 Analisis dan Hasil

4.2.1 Implementasi Tool

Tool berhasil diimplementasikan dengan baik mencangkup keseluruhan proses *scanning* jaringan Wi-Fi, akuisisi *hash* WPA2 melalui *4-Way Handshake*, konversi *file* ke format .hc22000, hingga proses *password cracking* menggunakan hashcat dalam satu aplikasi berbasis antarmuka GUI.

4.2.2 Pengujian Fungsional

Pengujian *tool* ini dilakukan pada beberapa skenario jaringan Wi-Fi dengan karakteristik berbeda. *4-Way Handshake* berhasil diperoleh dari jaringan dengan *client* aktif melalui serangan *deauthentication*. Proses *cracking password* menunjukkan efektivitas tinggi terhadap *passphrase* yang lemah atau umum ditemukan dalam wordlist.

4.2.3 Analisis Keamanan

Tool ini berhasil mendeteksi kerentanan jaringan Wi-Fi yang menggunakan *passphrase* statis dan tidak kompleks. Hasil *cracking* membuktikan bahwa penggunaan *password* sederhana masih sering dilakukan masyarakat umum,

sehingga meningkatkan risiko *eksploitasi*. Dengan *tool* ini, pengelola jaringan dapat lebih mudah melakukan evaluasi dan perbaikan konfigurasi keamanan.

4.2.4 Kelebihan dan Kekurangan Tools

Pada pengembangan *tool penetration testing* ini mendukung dua teknik akuisisi *hash*, yaitu dengan menggunakan dan *4-Way Handshake (deauthentucation)*. Perangkat ini terintegrasi *all-in-one* dengan penggunakan antarmuka GUI yang ramah pengguna. Di sisi lain, *tool penetration testing* ini memiliki kebergantungan pada kualitas *wordlist* untuk keberhasilan *cracking*.

Fitur	**Aplikasi Ini**	**aircrack-ng CLI**	**hcxtools + Hashcat (CLI)**
Integrasi GUI	Ya	Tidak	Tidak
Akuisisi Handshake	4-Way otomatis	4-Way handshake manual	PMKID capture manual
Wordlist Generator	Ya (custom & pattern-based)	Tidak	Tidak
Proses Otomatis End-to-End	Ya	Tidak	Tidak
Rata-rata Waktu Crack	10–15 menit	12–20 menit	8–12 menit
Kemudahan Penggunaan	Tinggi (GUI)	Rendah (CLI)	Sedang (CLI kompleks)

Table 2. Hasil Analisis

BAB V
PENUTUP

5.1 Kesimpulan

Penelitian ini berhasil mengembangkan sebuah *tool penetration testing all-in-one* berbasis GUI yang dapat digunakan untuk akuisisi dan *cracking* WPA2 menggunakan *4-Way Handshake*. Tool ini dibuat menggunakan Python dan PyQt5 yang dapat mengintegrasikan proses pemindaian, penangkapan *hash*, dan *cracking password* dalam satu antarmuka. Hasil pengujian menunjukkan bahwa tool efektif dalam mendeteksi kelemahan pada jaringan yang menggunakan passphrase lemah, dan dapat menjadi sarana edukasi serta audit keamanan yang praktis. Dengan adanya *tool* ini, proses pengujian keamanan jaringan Wi-Fi menjadi lebih efisien dan praktis, serta dapat berkontribusi pada peningkatan kesadaran dan kemampuan sumber daya manusia lokal dalam melakukan audit keamanan jaringan.

5.2 Saran

Berdasarkan hasil pengembangan *tool* ini, beberapa saran untuk pengembangan selanjutnya meliputi:

- Perluasan Cakupan Protokol: Mengembangkan kemampuan *tool* untuk mendukung protokol keamanan Wi-Fi yang lebih baru, seperti WPA3, atau jenis serangan nirkabel lainnya di luar *cracking password*.
- Peningkatkan Performa: Melakukan pengoptimalan lebih lanjut pada proses pemecahan *password* untuk meningkatkan kecepatan, misalnya dengan memanfaatkan sumber daya *cloud* atau integrasi dengan perangkat keras khusus yang lebih canggih.
- Fitur Lanjutan: Menambahkan fitur-fitur seperti analisis kerentanan otomatis, pembuatan laporan keamanan, atau integrasi dengan basis data *password* yang lebih besar dan terbarui.
- Fleksibilitas Platform (OS): Mengembangkan *tool* agar lebih portabel dan kompatibel dengan sistem operasi lain di luar Linux, seperti Windows atau macOS, untuk jangkauan pengguna yang lebih luas.

DAFTAR PUSTAKA

[1] S. Engebretson, *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*. Elsevier, 2013.

[2] K. Weidman, *Penetration Testing: A Hands-On Introduction to Hacking*, No Starch Press, 2014.

[3] V. Ramachandran and R. Buchanan, *BackTrack 5 Wireless Penetration Testing*, Packt Publishing, 2011.

[4] A. Herzog et al., "The Penetration Testing Execution Standard (PTES)," 2014.

[5] A. Bartoli et al., "Wireless Security in the Age of IoT," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 62-67, 2017.

[6] A. Nur and R. Saputra, "Analisis Keamanan Jaringan Wi-Fi Publik di Indonesia," *Jurnal Keamanan Siber*, vol. 3, no. 2, pp. 115-123, 2021.

[7] S. Mujawar et al., "Legal and Ethical Aspects of Penetration Testing," *International Journal of Computer Applications*, vol. 111, no. 15, pp. 1-5, 2015.

[8] S. Mujawar et al., "Legal and Ethical Aspects of Penetration Testing," *International Journal of Computer Applications*, vol. 111, no. 15, pp. 1-5, 2015.

[9] G. Tsitroulis et al., "A Survey on Security and Privacy Issues in Wireless Networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3431-3462, 2018.

[10] M. Vanhoef and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," in *Proc. ACM CCS*, pp. 1313-1328, 2017.

[11] C. Celosia and M. Cunche, "WPA2-Enterprise: The Forgotten Protocol," *IEEE Security & Privacy*, vol. 17, no. 3, pp. 54-62, 2019.

[12] P. Kohlios and T. Hayajneh, "Wi-Fi Security: WPA2 vs WPA3," *Future Internet*, vol. 10, no. 8, pp. 1-15, 2018.

[13] M. Rahman et al., "Security Threats in Wireless Networks," *IEEE Access*, vol. 7, pp. 97070-97090, 2019.

[14] S. Bhanot and R. Hans, "A Review and Comparative Analysis of Various Security Protocols in Wireless Networks," *International Journal of Computer Applications*, vol. 136, no. 7, pp. 1-6, 2016.

[15] J. Baek et al., "A Study on Password Cracking in WPA2-PSK Wireless Networks," *Journal of Information Security*, vol. 11, no. 2, pp. 89-98, 2018.

[16] Y. Yang et al., "GPU-Accelerated Password Cracking for WPA2-PSK," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1555-1567, 2019.

[17] J. Sýkora et al., "Analysis of WPA2 Security in Practice," *Journal of Network and Computer Applications*, vol. 104, pp. 1-10, 2018.

[18] D. Supriyanto, "Analisis Keamanan WPA2 di Lingkungan Kampus Indonesia," *Jurnal Teknik Informatika*, vol. 13, no. 1, pp. 45-52, 2022.

[19] Ahmad and Yaacob, "Deauthentication Attack Analysis on WPA2," *International Journal of Computer Science*, vol. 16, no. 5, pp. 101-107, 2019.

[20] J. Tian et al., "A Study on 4-Way Handshake Vulnerabilities in WPA2," *IEEE Access*, vol. 8, pp. 119045-119055, 2020.

[21] A. Putra et al., "Efektivitas Penangkapan 4-Way Handshake pada Jaringan Wi-Fi Kampus," *Jurnal Keamanan Informasi*, vol. 5, no. 2, pp. 67-74, 2021.

[22] J. Steube, "WPA2 PMKID Attack," 2018. [Online]. Available: https://hashcat.net/forum/thread-7717.html

[23] D. Zhao and W. Wang, "Evaluasi Efektivitas Teknik PMKID pada Access Point Modern," *Jurnal Keamanan Siber*, vol. 4, no. 1, pp. 33-41, 2021.

[24] B. Kurniawan et al., "Perancangan Aplikasi Penetration Testing Jaringan Wireless Menggunakan Python," *Jurnal Sistem Informasi*, vol. 16, no. 2, pp. 123-130, 2020.