Cyberspace: Jurnal Pendidikan Teknologi informasi
Volume 9, Nomor 2, Oktober 2025, hal. 89 – 97
ISSN 2598-2079 (print) | ISSN 2597-9671 (online)

Analisis Penggunaan *Fluxion portable* Untuk Menguji Wi-Fi Dengan Keamanan WPA/WPA2

Aulia Syarif Aziz[1], Reja Anggara Selian[1]

[1]Program Studi Pendidikan Teknologi Informasi
Universitas Islam Negeri Ar-Raniry Banda Aceh

Email: aulia.aziz@ar-raniry.ac.id

Abstract

With the convenience offered by Wi-Fi networks, cybercrimes targeting Wi-Fi passwords have become increasingly prevalent. This study aims to evaluate the effectiveness of using fluxion portable as a tool for testing the security of WPA/WPA2-protected Wi-Fi networks. The research was conducted on a ZTE-F609 router using an action research approach to gain deeper insights into the method's effectiveness. Fluxion portable operates by leveraging social engineering techniques, wherein attackers create a rogue access point that mimics the legitimate network. Through this social engineering method, unsuspecting users may enter their passwords on the rogue network. The findings indicate that fluxion portable is indeed effective in obtaining Wi-Fi passwords via psychological manipulation, which often goes unnoticed by users. These results highlight significant risks faced by Wi-Fi users, especially in environments lacking additional protections. To mitigate the potential threat of fluxion portable attacks, users are advised to hide their Wi-Fi network from public view or to use routers with enhanced security features, such as whitelist options. These recommendations are expected to improve Wi-Fi security and raise user awareness of existing potential threats.

Keywords: *Fluxion portable*, *network security, wifi security*

Abstrak

Dengan kemudahan yang ditawarkan oleh jaringan Wi-Fi, kejahatan siber berupa pembobolan *password* Wi-Fi menjadi semakin marak. Studi ini bertujuan untuk mengevaluasi efektivitas penggunaan *fluxion portable* sebagai alat uji keamanan Wi-Fi yang dilindungi WPA/WPA2. Penelitian dilakukan pada router ZTE-F609 menggunakan pendekatan action research untuk memberikan pemahaman yang lebih mendalam mengenai efektivitas metode ini. *Fluxion portable* bekerja dengan memanfaatkan teknik social engineering, di mana penyerang menciptakan jaringan palsu (rogue AP) yang menyerupai jaringan asli. Melalui rekayasa sosial ini, pengguna tanpa sadar memasukkan kata sandi mereka pada jaringan palsu tersebut. Penelitian ini menunjukkan bahwa *fluxion portable* terbukti efektif dalam

memperoleh kata sandi Wi-Fi melalui manipulasi psikologis yang umumnya tidak disadari pengguna. Hasil ini mengindikasikan risiko signifikan yang dihadapi pengguna Wi-Fi, terutama di lingkungan yang tidak memiliki perlindungan tambahan. Sebagai langkah mitigasi terhadap potensi serangan menggunakan *fluxion portable*, pengguna disarankan untuk menyembunyikan jaringan Wi-Fi mereka dari publik atau menggunakan *router* dengan fitur keamanan tambahan, seperti *whitelist*. Rekomendasi ini diharapkan dapat meningkatkan keamanan jaringan Wi-Fi serta kesadaran pengguna terhadap potensi ancaman yang ada.

Kata kunci: *Fluxion portable*, *keamanan jarigan, keamanan wifi*

1. Pendahuluan

Perkembangan teknologi yang cepat mendorong semakin tingginya kebutuhan akan akses internet dengan mobilitas yang tinggi dalam kehidupan sehari-hari. Hal ini tercermin dari banyaknya layanan internet gratis berbentuk *hotspot* yang tersedia di berbagai tempat umum, yang memanfaatkan teknologi *wireless* LAN (WLAN). *Hotspot* adalah lokasi di mana pengguna dapat mengakses layanan internet, umumnya melalui jaringan WLAN yang terhubung dengan penyedia layanan internet [1].

Pada tahun 2021, jumlah pengguna internet di Indonesia mengalami peningkatan sebesar 11 persen dibandingkan tahun sebelumnya, yaitu dari 175,4 juta menjadi 202,6 juta pengguna [2]. Di Indonesia, terdapat banyak penyedia layanan internet. Berdasarkan Data Indonesia.id, Badan Pusat Statistik (BPS) mencatat ada 611 *internet service provider* (ISP) di Indonesia pada tahun 2021 [3]. *Provider* yang paling banyak digunakan adalah Indihome, yang menurut survei APJII pada tahun 2022, mendominasi pasar layanan *fixed broadband* dengan persentase pengguna mencapai 67,54% [4]. Di Aceh, pada tahun 2021, PT. Telkom, khususnya Indihome, memiliki 148.232 pengguna [5]. Menurut Quira.com, alasan utama orang memasang Wi-Fi di rumah adalah untuk mempermudah akses internet. Banyak orang juga memilih Wi-Fi karena kemudahan dan praktisnya penggunaannya [6].

Namun, kemudahan dalam penggunaan Wi-Fi ini juga memunculkan berbagai tindakan ilegal untuk mengakses jaringan tersebut. Meski menggunakan keamanan WPA/WPA2, jaringan Wi-Fi tetap rentan menjadi target para pelaku kejahatan siber. Salah satu metode yang digunakan oleh para pelaku untuk mendapatkan *password* Wi-Fi adalah dengan alat tambahan berupa *fluxion portable*. Tindakan ilegal ini berpotensi melanggar hukum dan dapat dikenakan sanksi tegas. Perlindungan data pribadi telah diatur dalam Undang-Undang ITE Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang menegaskan bahwa pemilik data pribadi berhak atas keamanan dan kerahasiaan data tersebut, serta bahwa setiap pengguna atau penyelenggara sistem elektronik bertanggung jawab atas data yang dikuasainya. Sanksi bagi pelanggar diatur dalam Pasal 27 Ayat 3 UU ITE yang menyatakan bahwa setiap

orang yang dengan sengaja dan tanpa hak mendistribusikan atau mentransmisikan data elektronik yang mengandung penghinaan atau pencemaran nama baik dapat dipidana dengan hukuman penjara maksimal 4 tahun dan atau denda hingga Rp750.000.000,- [7].

Untuk mengukur tingkat keamanan sistem yang melindungi data pribadi, salah satu metode yang dapat dilakukan adalah dengan menguji ketahanan sistem terhadap ancaman, seperti menggunakan *fluxion*. *Fluxion* adalah sebuah program yang dirancang untuk menguji keamanan jaringan nirkabel, termasuk jaringan dengan keamanan WPA/WPA2. Program ini memanfaatkan teknik Man in the Middle Attack untuk menyusup ke jaringan dan memperoleh *password* Wi-Fi target dengan cara menipu pengguna untuk memasukkan *password* mereka pada halaman login yang dibuat oleh penyerang, bukan dengan cara membobol sistem secara langsung [8][9]. *Fluxion* awalnya merupakan perangkat lunak, namun sekarang telah berkembang menjadi perangkat keras portabel yang lebih praktis untuk digunakan.

Oleh karena itu, peneliti tertarik untuk mengkaji penggunaan *fluxion portable* dalam menguji keamanan Wi-Fi dengan WPA/WPA2, dan merumuskan judul penelitian ini menjadi "Analisis Penggunaan *Fluxion portable* untuk Menguji Wi-Fi dengan Keamanan WPA/WPA2".

2. Metodologi Penelitian

Dalam penelitian ini, penulis menerapkan metode *Action Research* atau penelitian tindakan. Metode ini melibatkan peneliti sebagai bagian aktif dalam proses penelitian tersebut. Tahapan-tahapan yang dilakukan dalam metode tindakan ini antara lain:

1) *Diagnosing*
   Mendiagnosis kondisi sistem jaringan Wi-Fi yang akan diteliti.
2) *Action Planning*
   Merencanakan langkah-langkah yang akan diambil, termasuk merancang dan menguji sistem jaringan Wi-Fi.
3) *Action Taking*
   Melaksanakan rencana yang telah disusun, serta mengidentifikasi kelemahan dalam sistem jaringan Wi-Fi.
4) *Evaluating*
   Melakukan evaluasi terhadap hasil analisis yang dilakukan menggunakan *fluxion portable* untuk mengungkap *password* Wi-Fi yang memiliki sistem keamanan WPA/WPA2 [10].

Penelitian ini dilakukan dengan menggunakan alat dan bahan yang dapat dilihat melalui Tabel 1 berikut:

Tabel 1 Alat dan Bahan

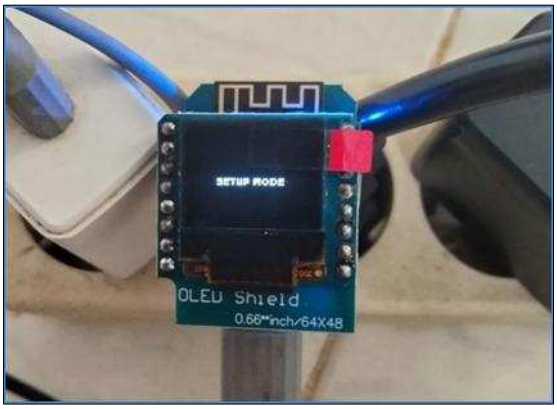
No	Nama	Spesifikasi	Jumlah	Fungsi
1	*Smartphone*	Android	2	Sebagai media untuk konfigurasi *fluxion*, mendeteksi, dan melakukan penyerangan pada Wi-Fi dengan keamanan WPA/WPA2.
2	*Router*	ZTE-F609	1	Sebagai pemancar sinyal Wi-Fi
3	*Fluxion*	*Fluxion portable*	1	Sebagai media penangkap, pemutus, dan pengambil *password* Wi-Fi.
4	USB	*Micro* USB		Sumber daya listrik untuk *Fluxion portable*
5	*Browser*	Chrome		Sebagai tempat pengujian dan juga melakukan *setting router* ZTE-F609.

3. Hasil dan Pembahasan

Penelitian ini mengkaji pengujian jaringan Wi-Fi dengan keamanan WPA/WPA2 menggunakan *fluxion portable*, serta alat pendukung lainnya, yang terdiri dari:

- 2 unit smartphone (satu sebagai target dan untuk mengonfigurasi router, dan satu lagi digunakan oleh penyerang untuk mencuri *password* Wi-Fi).
- 1 unit charger smartphone micro USB untuk menyediakan daya listrik bagi *fluxion portable*.
- *Fluxion portable* itu sendiri, yang digunakan untuk mencuri *password* Wi-Fi target.

Langkah pertama setelah menghidupkan *fluxion portable* adalah menghubungkannya ke sumber listrik menggunakan *charger smartphone*. Selanjutnya, konfigurasi dilakukan dengan menghubungkan *smartphone* penyerang ke Wi-Fi dengan nama SSID ATTRACTOR, yang merupakan nama jaringan dari *fluxion portable*. Setelah *smartphone* penyerang berhasil terhubung ke SSID *fluxion portable*, layar *fluxion portable* akan menampilkan pesan "SETUP MODE", yang menunjukkan bahwa alat tersebut siap digunakan, seperti yang dapat dilihat pada gambar 1.

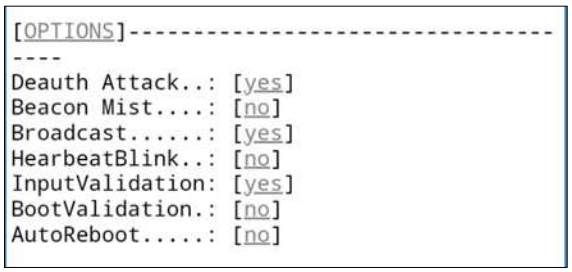


Gambar 1 *SETUP MODE* pada *fluxion portable*

Selanjutnya, konfigurasi *fluxion portable* dilakukan melalui browser Chrome dengan memasukkan alamat IP untuk halaman pengaturan *fluxion portable*, yaitu 192.168.4.1/setup. Kemudian, masukkan username "razor" dan *password* "admin" untuk *login* ke halaman pengaturan tersebut. Setelah berhasil login, pilih SSID atau nama Wi-Fi yang akan dijadikan target dengan menekan tombol "select" pada submenu *network* di menu TARGET pada halaman pengaturan *fluxion portable*, seperti yang terlihat pada gambar 2.

Gambar 2. Menu Target

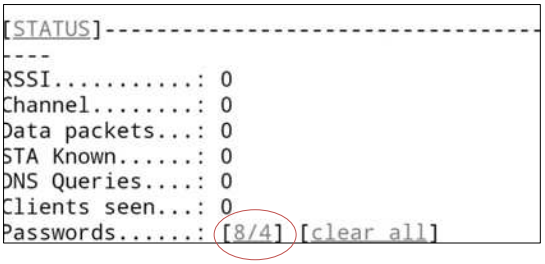
Selanjutnya pada sub menu *OPTIONS* tekan tombol *NO* untuk mengubahnya menjadi *YES*. Adapun pilihan yang harus diubah dari *NO* menjadi *YES* di sub menu *options* ini adalah *deauth attack* (memulai serangan dengan memutus semua perangkat yang terhubung pada Wi-Fi yang sudah dipilih menjadi target), *broadcas*t (mengirim SSID atau Wi-Fi tiruan yang hampir sama persis dengan aslinya), dan *input validation* (untuk memberikan perintah pada *fluxion portable* jika ada *password* yang dimasukkan akan dilakukan pengecekan langsung pada *router* ZTE-F609). Untuk tahapan ini dapat dilihat pada gambar 3.



Gambar 3 Menu *Options*

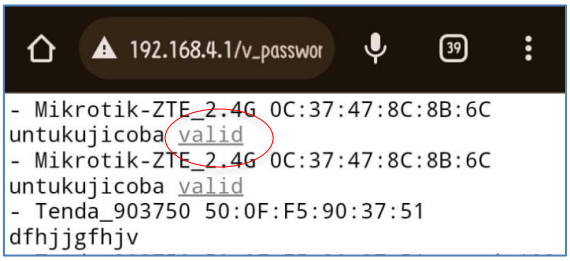
Untuk memulai serangan, langkah pertama adalah mematikan Wi-Fi pada *smartphone* penyerang. Setelah serangan dimulai, *smartphone* target akan terputus dari jaringan Wi-Fi dan dua jaringan dengan nama yang sama akan muncul, namun dengan jenis keamanan yang berbeda. Salah satu jaringan akan memiliki ikon gembok, sementara yang lainnya tidak. Wi-Fi dengan ikon gembok adalah jaringan asli, sedangkan Wi-Fi tanpa ikon gembok adalah jaringan palsu. Pada saat ini, Wi-Fi asli tidak dapat digunakan meskipun ada beberapa percobaan untuk menghubungkannya kembali.

Dalam keadaan bingung dan ragu, pengguna akan memilih untuk menghubungkan *smartphone* mereka ke jaringan Wi-Fi palsu. Begitu *smartphone* target terhubung dengan Wi-Fi palsu, perangkat tersebut akan diarahkan ke halaman *login* yang meminta *password* dari Wi-Fi target. *Smartphone* target akan terus diminta untuk memasukkan *password* hingga yang benar dimasukkan. Selama proses ini, satu-satunya pilihan yang tersedia adalah memasukkan *password* yang benar atau menunggu penyerang untuk menghentikan *fluxion portable* mereka. Setelah *password* yang benar dimasukkan, *smartphone* target akan terhubung ke Wi-Fi asli, dan Wi-Fi palsu akan berganti nama menjadi "ATTRACTHOR". *Password* yang berhasil diperoleh oleh *fluxion portable* dapat dilihat melalui submenu *passwords* di menu *STATUS*, seperti yang ditunjukkan pada gambar 4.



Gambar 4 Menu Status

Untuk mengetahui apakah *password* tersebut benar maka ada keterangan *Valid* di sebelah kanan *password* tersebut seperti yang terlihat pada gambar 5.



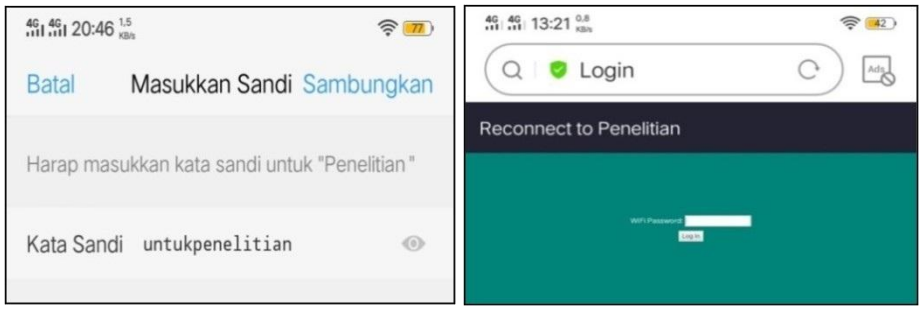
Gambar 5 Keterangan *Valid*

Berdasarkan langkah-langkah konfigurasi dan serangan menggunakan *fluxion portable* yang telah dijelaskan sebelumnya, berikut adalah informasi mengenai cara membedakan Wi-Fi asli dan Wi-Fi palsu:

1) Wi-Fi asli akan memiliki ikon gembok, sedangkan Wi-Fi palsu tidak memiliki ikon tersebut, seperti yang terlihat pada gambar 6.

Gambar 6 Ikon gembok pada Wi-Fi

2) Proses penghubungan antara Wi-Fi asli dan Wi-Fi palsu juga berbeda, sebagaimana ditunjukkan pada gambar 7.



Gambar 7 Perbedaan cara menghubungkan Wi-Fi

4. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa *Fluxion portable* efektif memutuskan koneksi semua perangkat yang terhubung ke Wi-Fi target setelah konfigurasi dan serangan dilakukan. Setelah perangkat terputus, tidak ada perangkat yang dapat terhubung kembali ke Wi-Fi target meskipun ada beberapa kali percobaan untuk menghubungkannya ulang. Dalam keadaan bingung dan panik, pengguna akan cenderung menghubungkan perangkat mereka ke Wi-Fi palsu, yang kemudian akan mengarahkan mereka ke halaman login untuk memasukkan *password* Wi-Fi. Jika pengguna memasukkan *password* yang benar, perangkat akan langsung terhubung ke Wi-Fi asli. Namun, jika *password* yang dimasukkan salah, pengguna akan diminta untuk mencoba memasukkan *password* yang benar hingga berhasil.

Keefektifan *fluxion portable* sangat bergantung pada situasi dan kondisi jaringan yang diuji. *Fluxion portable* akan lebih efektif untuk menguji jaringan Wi-Fi dengan keamanan WPA/WPA2, terutama di lingkungan dengan banyak pengguna non-IT dan jaringan Wi-Fi yang memiliki banyak pengguna aktif. Dalam penelitian ini, SSID Wi-Fi asli dan Wi-Fi palsu masih dapat dibedakan dengan jelas melalui ikon gembok yang ada di sebelah kanan SSID Wi-Fi asli, sementara Wi-Fi palsu tidak memiliki ikon tersebut. Perbedaan yang mencolok lainnya juga terlihat pada cara penghubungan, di mana Wi-Fi asli dan Wi-Fi palsu memiliki proses yang sedikit berbeda, serta perbedaan dalam alamat IP dan *gateway* yang digunakan.

Referensi

[1] Firmansyah, F., Bajili, I., Ahmadian, H., & Aziz, A. S. (2022). Implementasi Dan Analisis kinerja Antena Wajan Bolic Sebagai penerima Sinyal Wi-Fi. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *6*(2), 95-104.

[2] Aziz, A. S., & Safriatullah, S. (2021). Perancangan Dan Analisis Keamanan Pada Sistem Autentikasi Terpusat Freeradius. *Journal of Informatics and Computer Science*, *7*(2), 106-112.

[3] D. Bayu, "Ada 611 Perusahaan Penyedia *Internet* di Indonesia pada 2021," *DataIndonesia.id*, 2022. https://dataindonesia.id/*internet*/detail/ada-611-perusahaan-penyedia-*internet*-di-indonesia-pada-2021 (*accessed* Mar. 14, 2023).

[4] R. Hanif, "DIPSTATISTIK *INTERNET SERVICE PROVIDER* (*FIXED BROADBAND*) YANG PALING BANYAK DIGUNAKAN DI INDONESIA," *Blog Disptrategy*, 2022. https://dipstrategy.co.id/blog/dipstatistik-*internet*-service-provider-fixed-broadband-yang-paling-banyak-digunakan-di-indonesia/ (*accessed* Mar. 14, 2023).

[5] S. Sahat, M. Pasaribu, and R. Hidayat, "ANALISIS PERSONAL *SELLING* PRODUK INDIHOME PADA PT . TELKOM CABANG BANDA ACEH TAHUN 2021," vol. 7, no. 5, pp. 1039–1043, 2021.

[6] O. Situngkir, "Apa alasan orang memasang Wi-Fi?," *Quora.com*, 2020. https://id.quora.com/Apa-alasan-orang-memasang-Wi-Fi (*accessed* Mar. 14, 2023).

[7] Pemerintah Indonesia, "Undang-Undang No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik", Jakarta : Lembaran Negara RI, No.115, Jakarta, 2008.

[8] D. N. Widiatama, "ANALISA UJI KEAMANAN WPA2 MENGGUNAKAN *FLUXION* PADA PT. ANDAGLOS GLOBAL TEKNOLOGI," Institut Informatika Dan Bisnis Darmajaya, 2019

[9] V. Kumar, "*Fluxion* di Kali Linux digunakan untuk peretasan WPA WPA2 dalam hitungan menit Panduan Pemula," CyberPratibha. 2023. Available: https://www.cyberpratibha.com/blog/fluxion-wpa-wpa2-hacking/

[10] B. Suroto, "Metode penelitian tindakan solusi bagi masalah sosial," *Manaj. Pendidik. dan Pelatih.*, vol. 1, no. 1, pp. 25–28, 2017.