(2024), 2 (11): 176–192 **Scientica** 3021-8209

Jurnal Ilmiah Sains dan Teknologi

ANALISIS KEAMANAN JARINGAN PADA *ROUTER HUAWEI HG8245H5* DAN *REPEATER MERCUSYS MW300RE* MENGGUNAKANWI-FI *DEUTHER* UNTUK UJI KEAMANAN WPA2/PSK DENGAN METODE *PENETRATION TESTING*

Rian Febriyana, Yusuf Muhyidin, Dayan Singasatia
Program Studi Teknik Informatika S1, Fakultas Teknik,
Sekolah Tinggi Teknologi Wastukancana
Jl. Cikopak No.53, Sadang, Purwakarta, Jawa Barat, Indonesia

Abstract (English)
In today's era, everyone is required to engage in various online activities, from work and education to informal matters, all relying on the internet. To reduce individual data expenses, most households have installed Wi-Fi. Despite this, unauthorized users still attempt to access Wi-Fi without permission from the owner. Therefore, this study aims to analyze network security at Surya Jaya Per Company using Wi-Fi Deauther and Penetration Testing methods. Wi-Fi Deauther is a tool used to attack network security on routers, while Penetration Testing is a standard framework providing comprehensive guidelines for conducting penetration tests. In this case study, the researcher attempted to breach the WPA2/PSK security on routers and repeaters at Surya Jaya Per Company. The analysis results indicate that the researcher successfully attacked the WPA2/PSK network security and obtained the password. The researcher concludes that WPA2/PSK network security still has vulnerabilities, thus making it susceptible to attacks using Wi-Fi Deauther.

Article History
Submitted: 15 July 2024
Accepted: 24 July 2024
Published: 25 July 2024

Key Words
Network Security, Wi-Fi Deauther, Penetration Testing, Surya Jaya Per

Abstrak (Indonesia)
Pada masa sekarang, semua orang diharuskan untuk berkegiatan serba internet, mulai dari kerja, belajar mengajar hingga masalah *non* formalpun harus menggunakan internet. Setiap rumah kebanyakan telah terpasang Wi-Fi guna untuk mengurangi pengeluaran dana pembelian paket data per-orangannya. Walaupun permasalahannya, tetap saja ada *user* ilegal yang ingin menggunakan Wi-Fi untuk internetan tanpa izin pemiliknya. Maka dari itu penelitian ini bertujuan untuk menganalisis keamanan jaringan di Perusaan Surya Jaya Per dengan menggunakan Wi-Fi *Deauther* dan metode *Penetration Testing*. Wi-Fi *Deauther* adalah alat yang digunakan untuk menyerang keamanan jaringan terhadap *router*, sedangkan *Penetration Testing* adalah kerangka kerja standar yang memberikan panduan lengkap dalam melaksanakan uji penetrasi. Dalam studi kasus ini, penulis berusaha menyerang keamanan WPA2/PSK pada *router* dan *repeater* di Perusahaan Surya Jaya Per. Hasil analisis menunjukan bahwa peneliti berhasil melakukan penyerangan keamanan jaringan WPA2/PSK dan mengambil *password* tersebut. Peneliti menyimpulkan bahwa keamanan jaringan WPA2/PSK masih memiliki kerentanan, maka dari itu bisa di serang menggunakan Wi-Fi Deauther.

Sejarah Artikel
Submitted: 15 July 2024
Accepted: 24 July 2024
Published: 25 July 2024

Kata Kunci
Keamanan Jaringan, Wi-Fi *Deauther*, *Penetration Testing*, Surya Jaya Per

PENDAHULUAN

Pada masa sekarang kemajuan teknologi komunikasi merupakan faktor yang paling penting terhadap peranan masyarakat untuk mendapatkan akses informasi. Semua orang sangat membutuhkan jaringan internet yang mengharuskan untuk pelajar, mahasiswa, guru, dosen, pekerja kantoran dan lain sebagainya untuk beraktifitas. Aktifitasnya meliputi : kerjaan kantor, proses belajar mengajar, dan sebagainya. Tidak hanya kegiatan yang bersifat formal saja, bahkan hampir semua aktifitas di luar rumah menggunakan internet. Tidak menutup kemungkinan banyak rumah yang telah menggunakan WI-FI dalam meminimalisasi

pengeluaran dana untuk pembelian paket internet bulanan per orangnya untuk melakukan aktifitas internet yang mana bertujuan untuk memenuhi kebutuhan hidup yang berlangsung. Dengan adanya WI-FI banyak orang dapat melakukan aktifitas di internet dengan gratis tanpa membeli paket data per orangnya. Dikarenakan *wireless fidelity* (WI-FI) adalah standar untuk komunikasi *wireless* jarak pendek, terutama digunakan oleh komputer dan perangkat seluler. *wireless* atau WI-FI adalah jaringan yang menghubungkan telekomunikasi perangkat satu dengan yang lainnya, tanpa menggunakan media kabel sebagai media penghantarnya. Sebagai gantinya, jaringan nirkabel yang digunakan adalah media transmisi untuk mengantarkan gelombang elektromagnetik.(Prasetyo & Windranata, 2022)

Apabila jaringan komputer membutuhkan kabel jaringan seperti kabel *fiber optic*, dan *UTP*, jaringan nirkabel *wireless* hanya memanfaatkan gelombang *elektromagnetik* untuk mengirimkan sinyal dari perangkat satu ke perangkat lainnya. Salah satu keunggulan menggunakan jaringan *wireless* adalah kemudahan pemasangan. Jenis-jenis perangkat yang menggunakan *wireless*, seperti *wireless LAN*, telepon genggam, telepon *cordless*, satelit televisi, perangkat komputer dan laptop, *remote control*, hingga *GPS* yang berfungsi sebagai navigasi. Tetapi walaupun WI-FI sangat mudah digunakan, pasti ada orang-orang yang masih mengakses WI-FI dengan ilegal guna untuk akses internet tanpa memasang WI-FI di tempatnya. Mengakses internet dengan memutus dan mengirimkan *SSID* (nama WI-FI) palsu agar dapat terhubung pada WI-FI yang dituju. *Evil Twin* adalah *Service Set Identifier* (SSID) palsu yang meniru jaringan WI-FI asli. Tiruan ini benar-benar sangat mirip dengan *SSID* aslinya. Mulai dari nama, kekuatan sinyal, hingga *frekuensinya*. Pengguna bisa saja menyambungkan perangkatnya ke WI-FI *Evil Twin* ini karena mengira itu adalah WI-FI yang asli. *Evil Twin* ini bekerja dengan menggunakan teknik penyerangan bernama *man-in-the-middle* (MITM). Teknik ini memungkinkan pengguna *Evil Twin* untuk menyuntikan *malware* atau *Backdoor*. Salah satu praktek *Evil Twin* terpopuler kepada perangkat pengguna tanpa terdeteksi sama sekali. *Malware* tersebut lalu bisa digunakan untuk berbagai macam hal sesuai keinginan penyerang. Pengguna diarahkan kehalaman login palsu, entah itu login media sosial, login email, atau sekedar login untuk menggunakan WI-FI tersebut. Pengguna yang tidak tahu mengira bahwa itu adalah kolom login normal dan mengisi *username* serta *password* mereka tanpa rasa curiga. Walaupun paktanya, mereka baru saja menyerahkan informasi penting kepada *hacker* secara sukarela. Seiring berkembangnya teknik untuk menyerang keamanan *wireless*, diantaranya *brute force*. *Deltaxflux* mengembangkan sebuah program diberi nama *fluxion* untuk mendapatkan *password wireless* tanpa menggunakan teknik *brute force* seperti pada umumnya yang mana *fluxion* adalah sistem keamanan dan alat penelitian rekayasa sosial, yang mana bertujuan untuk membuat rekayasa sosial untuk mengambil kunci WPA2/PSK pada titik akses tersebut.(Studi et al., 2018)

Surya Jaya Per bergerak dibidang suku cadang mobil seperti *colt diesel, truk tronton* dan mobil besar yang lainnya. Surya jaya per berada di kecamatan sukatani kabupaten purwakarta, perusahaan ini membangun jaringan baru yang terdiri dari 2 (dua) perangkat *wireless* yang mencakup seluruh area kantor dengan menggunakan keamanan WPA2-PSK. *Wireless local area network* (WLAN) yang digunakan lebih sering mengalami kendala pada sistem keamanan jaringan dibandingkan menggunakan jaringan LAN. perangkat yang ada di Surya Jaya Per itu sendiri masih dalam tahap pembangunan jaringan baru, sehingga tingkat keamanan yang ada masih rentan dalam peretasan oleh pihak asing dan peneliti akan melakukan penelitian yaitu melakukan peretasan terhadap perangkat jaringan *wireless local area network* dan mengeksploitasi untuk memberikan solusi jika serangan berhasil dilakukan.

KAJIAN PUSTAKA

Jaringan Komputer

Jaringan komputer merujuk pada sekelompok perangkat yang terhubung, saling berinteraksi melalui standar komunikasi, menggunakan medium komunikasi. Dalam kerangka ini, perangkat dapat berbagi data, aplikasi, serta *periferal* seperti pencetak dan penyimpanan data. Jaringan komputer terbentuk dari komponen – komponen seperti mesin, perangkat jaringan, dan perangkat lunak yang bekerja bersama dalam satu ekosistem yang dikenal sebagai jaringan. Pemanfaatan jaringan komputer telah menjadi vital di dunia pendidikan, dimana lembaga – lembaga pendidikan memanfaatkannya untuk mendukung proses belajar mengajar. Oleh karena itu, manajemen yang baik terhadap infrastruktur jaringan sangatlah penting untuk memastikan kinerjanya tetap optimal menurut Deagama, 2022.(Putra, 2024).

Keamanan Jaringan

Keamanan jaringan adalah proses untuk mengidentifikasi dan mencegah pengguna yang tidak sah dari suatu jaringan komputer. Tujuannya tentu saja mengantisipasi resiko ancaman berupa perusakan bagian fisik komputer maupun pencurian data seseorang.(Soesanto et al., 2023).

Wireless Fidelity (Wi-Fi)

WI-FI adalah teknologi jaringan nirkabel yang memungkinkan perangkat seperti komputer (laptop dan dekstop), perangkat seluler (ponsel pintar dan perangkat yang dapat dikenakan), dan peralatan lain (printer dan kamera video) untuk berinteraksi dengan internet. Hal ini memungkinkan perangkat ini untuk bertukar informasi satu sama lain, menciptakan jaringan. Konektivitas internet terjadi melalui *router* nirkabel. Saat Anda mengakses WI-FI, Anda terhubung ke perute nirkabel yang memungkinkan perangkat Anda yang kompatibel dengan WI-FI untuk berinteraksi dengan internet.(Saidah & Hairunnisa, 2023).

WPA2/PSK

WPA2/PSK merupakan level keamanan yang paling tinggi. Enkripsi utama yang digunakan pada WPA2/PSK ini enkripsi AES. AES mempunyai kerumitan yang lebih tinggi daripada RC4 pada WEP sehingga para vendor tidak sekedar *upgrade* firmware seperti dari WEP ke WPA. Untuk menggunakan WPA2/PSK diperlukan hardware baru yang bekerja dengan lebih cepat dan mendukung perhitungan yang dilakukan oleh WPA2/PSK, sehingga tidak semua adapter mendukung level keamanan WPA2/PSK ini. Pada *security* mode WPA2-PSK ada dua pilihan enkripsi pada jenis ini, yaitu TKIP dan AES.

1. TKIP (*Temporal Key Integrity Protocol*) menggunakan metode enkripsi yang lebih aman dan juga menggunakan MIC (*Message Integrity Code*) untuk melindungi jaringan dari serangan.
2. AES (*Advanced Encryption System*) menggunakan enkripsi 128 bit blok data secara simetris. Untuk menggunakan WPA *Pre-Shared Key*,masukkan *password* pada WPA *Shared Key* dengan panjang karakter 8 sampai 63. *Group Key Renewal Interval* diisi dengan nilai *default* yaitu 3600 *seconds*.

WI-FI *Protected Acces* versi 2 (WPA2/PSK) adalah sebuah *protokol kriptografi* yang berfungsi untuk mengamankan jaringan *wireless*. WPA2/PSK diperkenalkan oleh WI-FI *Alliance* pada tahun 2004. WPA2/PSK memenuhi syarat standar yang ditetapkan oleh *IEEE 802.1 1i.* Dalam metode pengamanan WPA2/PSK menggunakan algoritma *AES* sebagai

proses *enkripsi* dan *CBC-MAC* sebagai proses *enkripsi traffic* pada jaringan dan melindungi integritas data.(Darma et al., 2022).

Wi-Fi Deauther

Deauther atau *jammer* dalam dunia telekomunikasi yaitu sebuah alat yang digunakan untuk memutus hubungan komunikasi perangkat telekomunikasi. WI-FI deauther bekerja dengan 2 mode serangan secara bersamaan yaitu memutuskan koneksi device yang terhubung ke *acces point* atau *router* dan juga membuat *SSID* atau WI-FI palsu sebagai *captive portal*.(Aman, 2023)

Fluxion

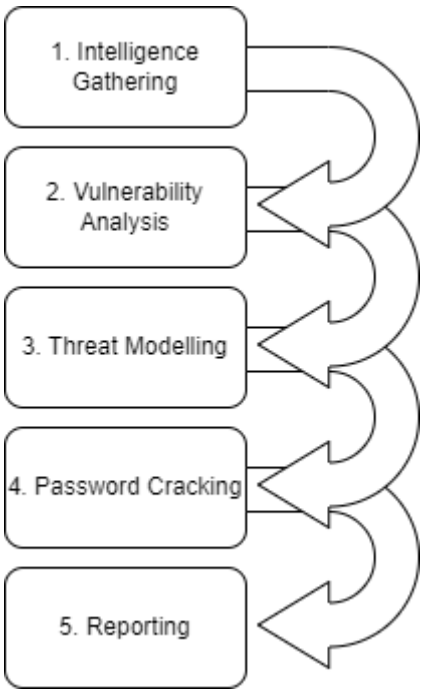
Fluxion adalah *audit* keamanan dan alat penelitian rekayasa sosial. Ini adalah *remake* (pembuatan ulang) dari alat *linset* oleh *vk496* dengan (semoga) lebih sedikit bug dan banyak fungsionalitas. *Script* mencoba untuk menganbil kunci WPA2/PSK dari titik akses target melalui serangan rekayasa sosial (*phishing*).(Muhammad et al., 2023)

Cara kerja :

1. Pindai jaringan nirkabel target.
2. Luncurkan serangan *Handshake Snooper*.
3. Tangkap jabat tangan (diperlukan untuk *verifikasi* kata sandi).
4. Luncurkan serangan *Captive Portal*.
5. Memunculkan acces point palsu, meniru titik akses asli.
6. Memunculkan server DNS, mengarahkan semua permintaan ke *host* penyerang yang menjalankan portal tawanan.
7. Memunculkan server web, melayani portal tawanan yang meminta pengguna memasukkan kunci WPA/WPA2 mereka.
8. Memunculkan *jammer*, menonaktifkan *client* dari *acces point* asli dan memikat mereka ke *acces point* palsu.
9. Semua upaya otentikasi di *portal* tawanan diperiksa terhadap *file* jabat tangan yang diambil sebelumnya.
10. Serangan akan secara otomatis berhenti setelah kunci yang benar telah dikirimkan.
11. Kunci akan dicatat dan *client* akan diizinkan untuk terhubung kembali ke titik akses target.

Penetration Testing

Penetration testing atau uji *penetrasi* adalah sebuah upaya untuk mengetahui kelemahan dari sistem informasi dengan tujuan agar sistem informasi tersebut lebih aman dengan secara legal dan berwenang. *Penetration testing* merupakan suatu kegiatan berupa simulasi yang dilakukan oleh pihak yang sudah memiliki ijin untuk melakukan eksploitasi suatu sistem berdasarkan celah keamanan yang ada. *Penetration testing* berbeda dengan *hacking*, dimana kegiatan *hacking* tidak memiliki ijin untuk melakukan serangan terhadap sistem tersebut. Tujuan dari *penetration testing* adalah untuk mengidentifikasi kerentanan dalam sistem keamanan. Pengujian *penetrasi* dapat digunakan untuk pengujian kebijakan keamanan sistem yang terdapat pada perusahaan atau organisasi untuk melakukan identifikasi dan penanganan jika masalah tersebut mengancam keamanan sistem. Proses *penetration testing* terdiri dari pengumpulan informasi, identifikasian celah - celah keamanan, dan melakukan pelaporan terhadap hasil dari pengujian yang dilakukan.(Andriyani et al., 2023)

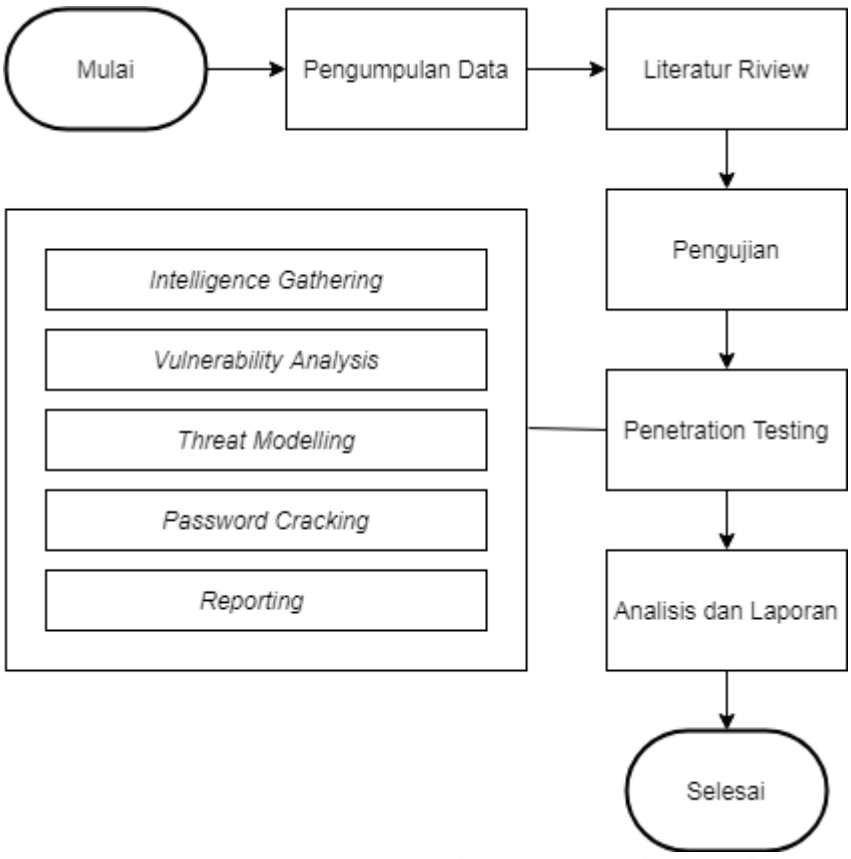


Gambar 1 Alur Penetration Testing

METODE

Kerangka Penelitian

Adapun kerangka penelitian yang akan dijalankan pada gambar 2 sebagai berikut :



Gambar 2 Kerangka Penelitian

Pengumpulan Data

Dalam proses pengumpulan data menggunakan metode kualitatif dengan menggunakan dua teknik yang dilaksanakan untuk mengumpulkan data-data yang diperlukan mengenai penelitian ini. Metode pengumpulan data terdiri sebagai berikut :

1. Wawancara

Peneliti melakukan pengumpulan data dengan melakukan komunikasi dengan pihak perusahaan Surya Jaya Per untuk menanyakan terkait hal yang diperlukan dalam penelitian .

2. Observasi

Observasi yang dilakukan peneliti yaitu melakukan pengamatan terhadap jaringan *router Huawei HG8245H5* dan *repeater Mercusys MW300RE* .

Literatur Riview

Studi literatur dalam penelitian ini yaitu dengan proses mempelajari jurnal penelitian terdahulu yang telah dilakukan dengan maksud untuk memperoleh teori-teori yang dibutuhkan dan sebagai landasan dilakukan nya kegiatan penelitian. *Studi literatur* dapat mengarahkan penelitian dalam menyusun kerangka penelitian yang jelas dan terarah sehingga penelitian memiliki *referensi* yang jelas dalam pemecahan masalahnya.

Pengujian

Adapun tahapan selanjutnya peneliti melakukan pengujian WPA2/PSK menggunakan Wi-Fi Deauther

Tahap pengujian ini memiliki 5 (lima) tahapan utama yang akan digunakan pada penelitian yaitu :

a. *Intelligence Gathering:*

Tahapan ini penguji mencoba mendapatkan informasi pada perangkat *wireless* dengan menggunakan Wi-Fi *Deauther* sehingga informasi bisa berupa *SSID, BSSID, Channel, RSSI, Encryption* dan *Change.*

b. *Vulnerability Analysis:*

Langkah ini penulis akan memutuskan jaringan Wi-Fi yang tersambung ke *Handphone* target menggunakan *tool Deauth Attack* yang ada di Wi-Fi *Deauther*.

c. Threat Modelling:

Informasi yang didapatkan sebelumnya telah mempermudah penguji untuk menganalisa dan menggunakan *tool Beacon Mist* untuk membuat *Fake SSID* yang terdapat di Wi-Fi *Deauther* sebagai serangan yang dimana akan memanipulasi *wireless* target.

d. Password Cracking:

Pada tahapan ini penguji melakukan *Deauth Attack, Beacon Mist, Input Validation dan Boot Validation* pada *fluxion tool* terhadap *user* yang terkoneksi dalam jaringan *wireless* yang telah di manipulasi sehingga penguji mendapatkan sebuah paket berupa kode untuk dipecahkan menjadi *password* sesuai dengan metode yang telah disiapkan dalam tahapan *Intelligence Gathering, Vulnerability Analysis* dan *Threat Modelling*.

e. Reporting

Reporting yaitu hasil akhir dari pengujian sistem. Penguji medokumentasikan hasil dari penelitian dalam bentuk sebuah laporan.

Penetration Testing yang akan dilakukan pada *fase* ini untuk melakukan penyerangan jaringan keamanan, dengan menggunakan 4 *tool* yaitu :

1. Deauth Attack

Deauth Attack digunakan untuk memutuskan jaringan target ke *router* dan *repeater*.

2. Beacon Mist

Beacon Mist digunakan untuk kloning *SSID* agar target masuk kedalam *SSID* palsu yang dibuat.

3. Input Validation

Input Validation digunakan untuk menginput *password* yang dimasukan oleh target agar terbaca di halaman web.

4. Boot Validation

Boot Validation digunakan untuk memberitahu *password* yang dimasukkan oleh target yang benar atau salah.

Analisis dan laporan

Pada tahap ini dilakukan analisis terhadap pengujian yang sudah dilakukan dan merangkumnya ke dalam sebuah laporan.

HASIL DAN PEMBAHASAN

Pengumpulan Data

Observasi

Hasil observasi yang dilakukan peneliti di Perusahaan Surya Jaya Per mengungkapkan bahwa perusahaan ini membangun jaringan baru yang terdiri dari 2 (dua) perangkat *wireless* yang mencakup seluruh area kantor dengan menggunakan keamanan WPA2/PSK. *Wireless local area network* (WLAN) yang digunakan lebih sering mengalami kendala pada 182ystem keamanan jaringan dibandingkan menggunakan jaringan LAN. perangkat yang ada di Surya Jaya Per itu sendiri masih dalam tahap pembangunan jaringan baru, sehingga tingkat keamanan yang ada masih rentan dalam peretasan oleh pihak asing dan peneliti akan melakukan penelitian yaitu melakukan peretasan terhadap perangkat jaringan *wireless local area network* dan mengeksploitasi untuk memberikan solusi jika serangan berhasil dilakukan.

Wawancara

Hasil wawancara kepada pemilik Perusahaan Surya Jaya Per menjelaskan bahwa perangkat yang ada di Surya Jaya Per itu masih baru dan bisa disebut jaringan baru,sehingga tingkat keamanan nya yang masih rentan. Maka dari itu pihak Surya Jaya Per memberikan ijin untuk penulis melakukan pengujian terhadap jaringan mereka.

Literatur Riview

Hasil dari studi pustaka yang peneliti lakukan untuk memperkuat penelitian ini adalah mencari mengenai konsep dan teknik dari buku, jurnal dan tugas akhir mengenai penyerangan menggunakan Wi-Fi *Deauther* dengan metode *Penetration Testing*.

Pengujian

Pengujian WPA2/PSK Menggunakan Wi-Fi Deauther

Penelitian ini membahas tentang uji coba keamanan WPA2/PSK yang mana dalam penelitiannya menggunakan alat – alat yang ada dibawah ini. Bisa dilihat pada tabel 4.1 sebagai berikut :

Tabel 1 Alat - alat

NO	Alat	Fungsi
1.	Laptop.	Alat penyerang target.
2.	Kabel USB.	Menyambungkan Wi-Fi *Deauther* ke laptop.
3.	Wi-Fi Deauther.	Untuk memutus dan mengambil *password* Wi-Fi

		target.
4.	Handphone.	Sebagai target.

Tahap pengujian keamanan WPA2/PSK menggunakan Wi-Fi *Deauther* :

1. Untuk memulai uji keamanan WPA2/PSK, hubungkan Wi-Fi *Deauther* dengan laptop menggunakan kabel *USB*. Bisa dilihat pada gambar 3 sebagai berikut :

Gambar 3 Wi-Fi *Deauther* menggunakan *USB*

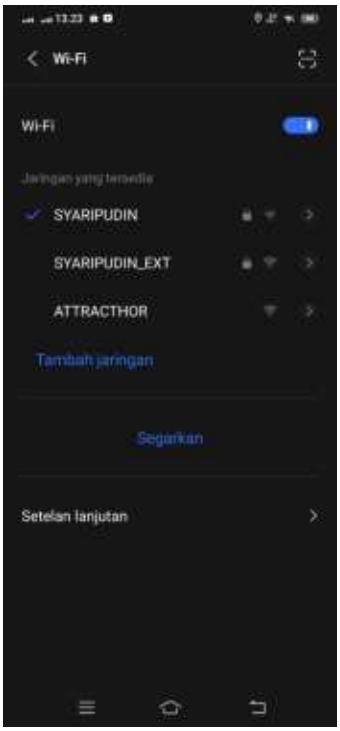
2. Hubungkan jaringan ke *SSID* Wi-Fi *Deauther* yang bernama *ATTRACTHOR* pada jendela *Wireless Network Connection*, dengan klik *SSID ATTRACTHOR*, *klik Connect*. Bisa dilihat pada gambar 4 sebagai berikut :

Gambar 4 Jendela *Wireless Network Connection*

Maka laptop terkoneksi dengan *SSID ATTRACTHOR*. Bisa dilihat pada gambar 5 sebagai berikut :

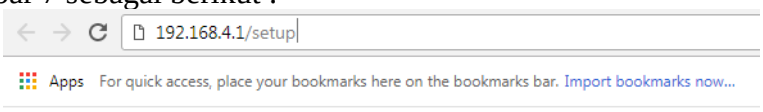
Gambar 5 *Connect ATTRACTHOR*

3.Kemudian pastikan *Handphone* terhubung pada *SSID router Huawei HG8245H5*. Bisa dilihat pada gambar 6 sebagai berikut :



Gambar 6 *Handphone* terkoneksi *router Huawei*

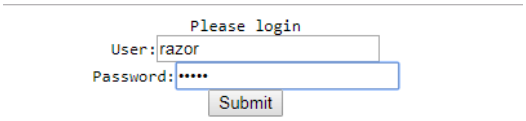
4.Kembali ke laptop, masuk ke *browser* dan ketik IP *192.168.4.1/setup* lalu tekan *enter*. Bisa dilihat pada gambar 7 sebagai berikut :



Gambar 7 Masukan *IP* di browser

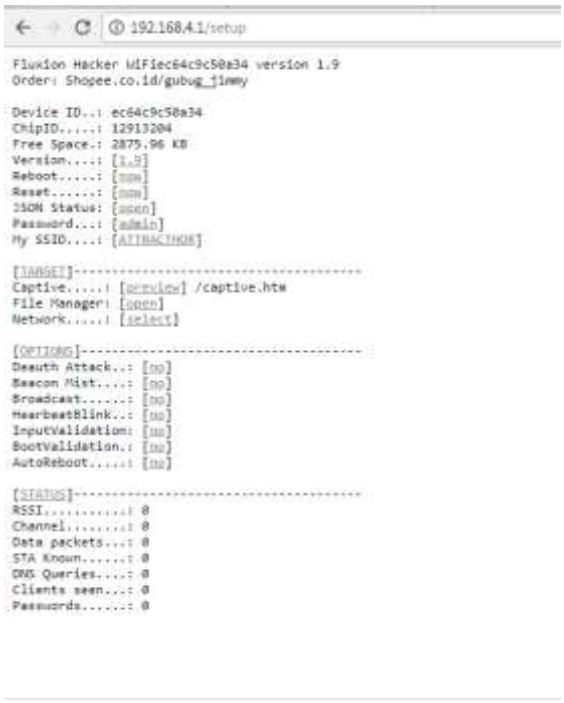
Kemudian akan muncul *form login* Wi-Fi *Deauther*, masukkan *user* : razor, sandi : admin lalu tekan *submit*. bisa dilihat pada gambar 8 sebagai berikut :

(2024), 2 (11): 176–192 Scientica 3021-8209
Jurnal Ilmiah Sains dan Teknologi



Gambar 8 Login Wi-Fi Deauther

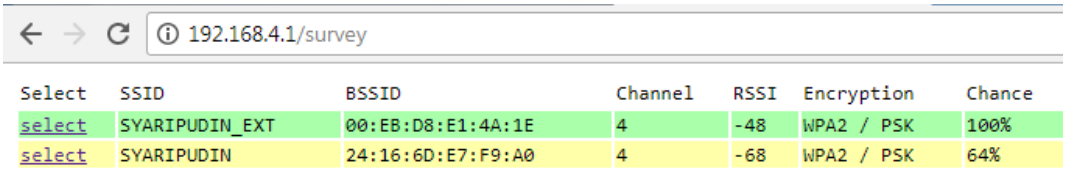
Maka akan muncul *Interface* Wi-Fi *Deauther*. Bisa dilihat pada gambar 9 sebagai berikut :



Gambar 9 *Interface* Wi-Fi *Deauther*

Intelligence Gathering

Pada tahap *Intelligence Gathering* penguji mencoba mendapatkan informasi pada perangkat *wireless* dengan menggunakan Wi-Fi *Deauther* sehingga informasi bisa berupa *SSID*, *BSSID*, *Channel*, *RSSI*, *Encryption* dan *Change*. Bisa dilihat pada Gambar 10 sebagai berikut :



Gambar 10 *Fase Intelligence Gathering*

Vulnerabillity Analysis

Pada tahap *Vulnerabillity Analysis* penguji akan memutuskan jaringan Wi-Fi yang tersambung ke *Handphone* target menggunakan *tool Deauth Attack* yang ada di Wi-Fi *Deauther*. Bisa dilihat pada gambar 11 sebagai berikut :

(2024), 2 (11): 176–192 Scientica 3021-8209
Jurnal Ilmiah Sains dan Teknologi

Gambar 11 *Fase Vulnerabillity Analysis*

Threat Modelling

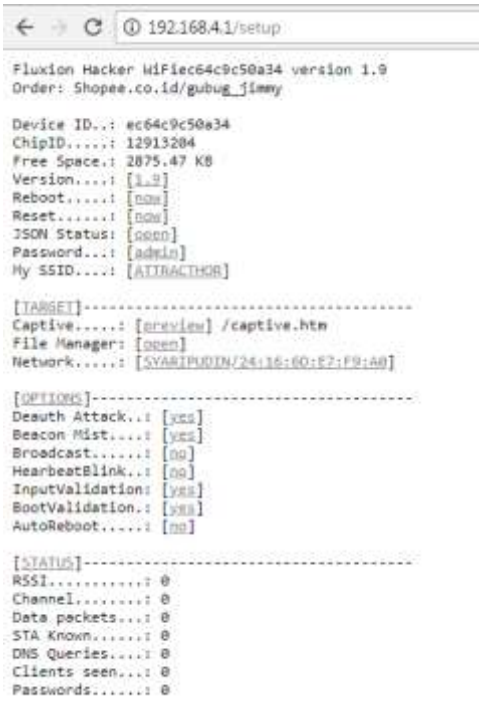
Pada tahap Threat Modelling penguji menggunakan *tool Beacon Mist* untuk membuat *Fake SSID* yang terdapat di Wi-Fi *Deauther* sebagai serangan yang dimana akan memanipulasi *wireless* target. Bisa dilihat pada gambar 12 sebagai berikut :

Gambar 12 *Fase Threat Modelling*

Password Cracking

Pada tahap Password Cracking penguji melakukan *Deauth Attack, Beacon Mist, Input Validation dan Boot Validation* pada *fluxion tool* terhadap *user* yang terkoneksi dalam jaringan *wireless* yang telah di manipulasi sehingga penguji mendapatkan sebuah paket berupa kode untuk dipecahkan menjadi *password* sesuai dengan metode yang telah disiapkan dalam tahapan *Intelligence Gathering, Vulnerability Analysis* dan *Threat Modelling.* Bisa dilihat pada gambar 13 sebagai berikut :

(2024), 2 (11): 176–192 Scientica 3021-8209
Jurnal Ilmiah Sains dan Teknologi

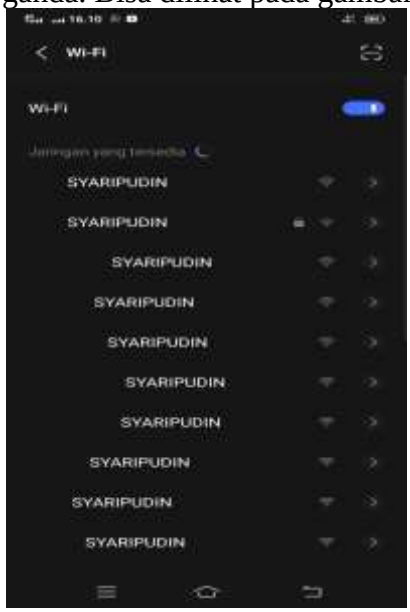


Gambar 13 *Fase Password Cracking*

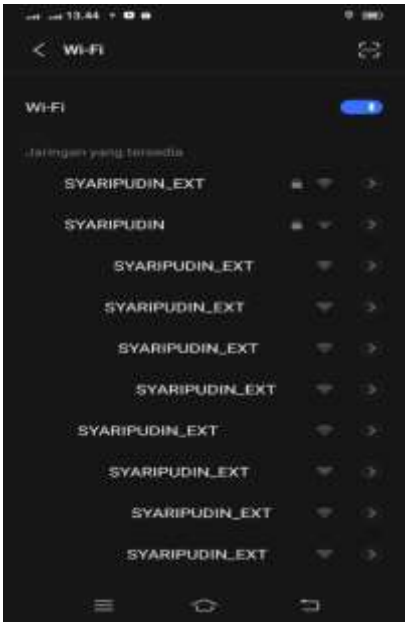
1. Memulai Serangan

a. Serangan Berhasil

Untuk memulai serangan putuskan *SSID ATTRACTHOR* pada laptop agar serangan dimulai. Setelah memulai serangan maka jaringan yang ada di *Handphone* akan terputus dan *SSID* yang sama akan menjadi ganda. Bisa dilihat pada gambar 14 dan 15 sebagai berikut :

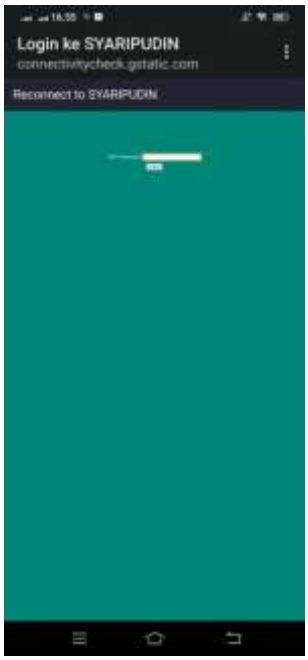


Gambar 14 Kloning *SSID Huawei*



Gambar 15 Kloning SSID Mercusys

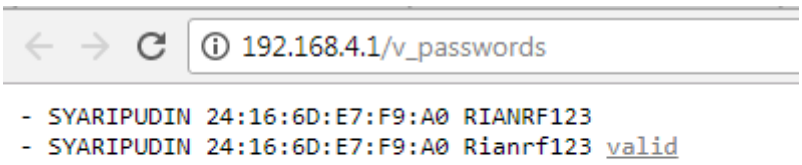
Bila target masuk ke *SSID* asli otomatis akan terputus terus, terpaksa target harus masuk ke *SSID* palsu, setelah klik *SSID* palsu target akan diarahkan kehalaman *form login* dan disuruh untuk memasukkan *password*, bila memasukkan *password* salah maka akan muncul *Interface Please wait* dan akan di arahkan kembali ke *form login*, bila memasukkan *password* yang benar akan muncul *Interface Please wait* lalu akan terkoneksi kembali ke *SSID* yang asli secara otomatis. Bisa di lihat pada gambar 16, 17 sebagai berikut :



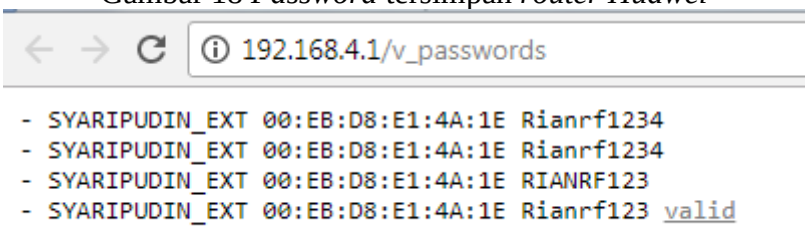
Gambar 16 *Interface masukkan password*

Gambar 17 *Interface Please wait*

Setelah memasukkan *password* yang benar target akan kembali *connect*, dan *password* pun terbaca oleh Wi-Fi *Deauther*. Bisa dilihat pada gambar 18 dan 19 sebagai berikut :



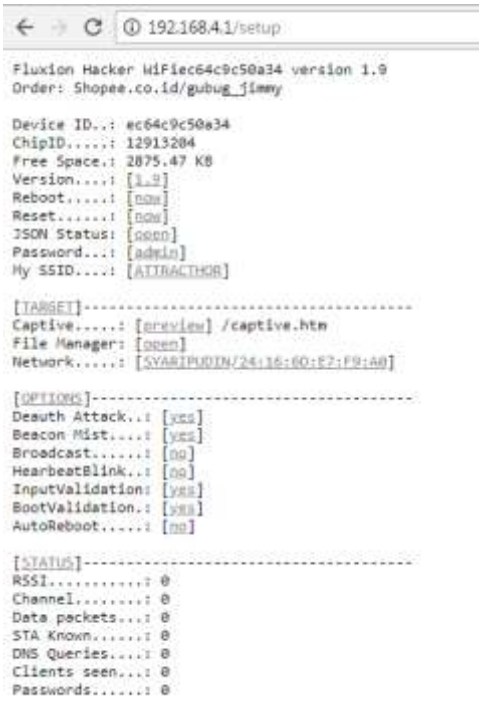
Gambar 18 *Password* tersimpan *router Huawei*



Gambar 19 Password tersimpan repeater Mercusys

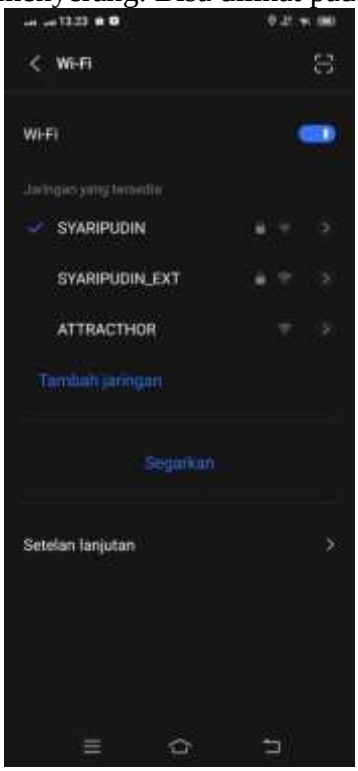
b. Serangan Gagal

Untuk memulai serangan putuskan *SSID ATTRACTHOR* pada laptop agar serangan dimulai. Apabila serangan gagal tidak akan terjadi pemutusan jaringan handphone oleh wi-fi *Deauther* dikarenakan serangan gagal dilakukan. Maka akan tetap di *Interface* tersebut. Bisa dilihat pada gambar 20 sebagai berikut :



Gambar 20 Gagal Menyerang

Bahkan *SSID ATTRACTHOR* pun tidak mengkloning *SSID* target dikarenakan gagal menyerang. Bisa dilihat pada gambar 21 sebagai berikut:



Gambar 21 Gagal *Kloning SSID*

Reporting

Pada tahap *Reporting* penguji medokumentasikan hasil dari penelitian dalam bentuk sebuah laporan.

Analisis dan Laporan

Pada tahap ini, peneliti telah membuat hasil dan analisis dari pengujian terhadap keamanan jaringan WPA2/PSK pada *router Huawei HG8245H5* dan *repeater Mercusys MW300RE* di Surya Jaya per sebagai berikut. Bisa dilihat pada Tabel 2 dan 3 sebagai berikut:

Tabel 2 Informasi hasil penyerangan

Jenis Serangan	Brute Force	Brute Force
Nama Perangkat	SYARIPUDIN	SYARIPUDIN_EXT
Tipe Keamanan	WPA2/PSK	WPA2/PSK
Informasi	Mendapatkan Password.	Mendapatkan Password.
Status	1. Berhasil 2. Gagal Menyerang	1. Berhasil 2. Gagal Menyerang

Tabel 3 Data log penyerangan

Penyerangan	Jenis Serangan	Target Pengujian	Tgl/Hari/Waktu	Hasil yang didapatkan
Pengujian 1	Brute force	Huawei HG8245H5	17 April 2024/5 menit	Berhasil mendapatkan password
Pengujian 2	Brute force	Huawei HG8245H5	17 April 2024	Gagal Menyerang
Pengujian 3	Brute force	Mercusys MW300RE	17 April 2024/7 menit	Berhasil mendapatkan password
Pengujian 4	Brute force	Mercusys MW300RE	17 April 2024	Gagal Menyerang

KESIMPULAN

Berdasarkan pembahasan yang sudah dipaparkan pada penelitian ini yang berjudul analisis keamanan jaringan pada *router Huawei HG8245H5* dan *Repeater MERCUSYS MW300RE* menggunakan Wi-Fi *Deuther* untuk uji keamanan WPA2/PSK dengan metode *Penetration Testing*, maka dapat disimpulkan sebagai berikut :

1. Pada *script fluxion* proses pengambilan *password* sangat berpengaruh, jika *password* tidak ditemukan proses kerja *script* tidak akan berhasil, dan pada Wi-Fi minimal mempunyai satu user yang sedang login karena *password* didapatkan oleh *user* yang sedang melakukan aktivitas pada jaringan tersebut.
2. Awalan *Handphone* yang terhubung akan terputus terlebih dahulu. Kemudian *SSID* telah menjadi ganda, maka target akan kebingungan dan memilih salah satu dari *SSID*, jika terpilih *SSID* palsu maka akan dialihkan langsung dengan login dari *SSID* palsu, setelah memasukkan *password* target akan otomatis terhubung dengan jaringan internet sebelumnya dan jika target login menggunakan *SSID* asli maka sambungan internet akan terputus terus menerus.
3. Keamanan jaringan WPA2/PSK pada *router Huawei HG8245H5* dan *repeater Mercusys MW300RE* masih bisa di tembus oleh Wi-Fi *Deauther*.

DAFTAR PUSTAKA

Prasetyo, S. E., & Windranata, T. (2022). Perbandingan Sistem Autentikasi Wpa2 Eap-Psk Pada Jaringan Wireless Dengan Metode Penetration Testing Menggunakan Fluxion Tools. *Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab*, *7*(1), 43–51. https://doi.org/10.36341/rabit.v7i1.2206

Studi, P., Informatika, T., & Batam, U. P. (2018). *KEAMANAN JARINGAN NIRKABEL DENGAN METODE EVIL TWIN ATTACK PADA KALI LINUX*.

Putra, R. P. (2024). *analisis kinerja jaringan LAN di laboratorium SMK Wiyata Satya Menggunakan metode quality of service (QOS)*. *3*(1).

Soesanto, E., Saputra, F., Puspitasari, D., & Putra Danaya, B. (2023). Determinasi Sistem Manajemen Sekuriti: Analisis Objek Vital, Pengamanan File dan Pengamanan Cyber pada Yayasan Siber Publisher. *Jurnal Ilmu Multidisiplin (JIM)*, *2*(1), 23–29. https://creativecommons.org/licenses/by/4.0/

Saidah, E. D., & Hairunnisa, K. M. B. (2023). *Implementasi Program "Wifi Smart" Dalam Pemanfaatan Teknologi Digital Pelajar Di Kelurahan Lok Tuan Kota Bontang*. *11*(3), 108–117.https://ejournal.ilkom.fisip-unmul.ac.id/site/wp-content/uploads/2023/06/Ejournal Implementasi Program Wifi Smart (ENDANG DWI SAIDAH 1602055032) (06-21-23-02-

Darma, U. B., Pangestu, K., Komputer, T., Vokasi, F., Darma, U. B., Informatika, T., Teknologi, F. S., & Darma, U. B. (2022). *Implementasi Virtual Private Network Dan Pembatasan Mac Address Pada Pt Pegadaian Kantor*. 57–64.

Aman, A. (2023). Pengujian Keamanan Jaringan Nirkabel Melalui Simulasi Serangan Man In The Middle Attack Di Sekolah XYZ. *Digital Transformation Technology*, *3*(2), 824–831. https://doi.org/10.47709/digitech.v3i2.3378

Muhammad, L., Fikri, Z., Zafrullah, A., & Zubaidi, A. (n.d.). *Analisis Keamanan Jaringan Wi-Fi Dengan Metode Deauthentication Attack Pada Access point Di Lingkungan Universitas Mataram (Wi-Fi Network Security Analysis With Deauthentication Attack Method At Access point In The University Of Mataram)*.

Andriyani, S., Sidiq, M. F., & Zen, B. P. (2023). Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar. *Journal Informatic and Information Technology*, *8798*, 1–13.