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)*

Lalu Muhammad Zahirul Fikri[1], Ahmad Zafrullah M[1], Ariyan Zubaidi [1]
[1]Dept Informatics Engineering, Mataram University
Jl. Majapahit 62, Mataram, Lombok NTB, INDONESIA
Email: Fikrizahirul30@gmail.com, [zaf, zubaidi13]@unram.ac.id

Wi-fi networks are not only used by individuals, but also by agencies, organizations, universities to government or non-government institutions, one of which is at the University of Mataram college. Today, there are various types of attacks on Wi-Fi network access called Denial of Service (DoS). One type of attack that can occur with an impact that is quite disturbing to the comfort of wi-fi network users is Deauthentication Attack. The study aims to be able to determine the percentage of the number of wi-fi networks on access points that are vulnerable and not vulnerable to the Deauthentication Attack method in the University of Mataram environment, and can find out the causes of wi-fi networks at access points that are vulnerable and not vulnerable to the Deauthentication Attack method in the University of Mataram environment with the hope that this research can be a reference or reference in installing access points for parties University of Mataram to avoid the impact of Deauthentication Attack. Based on the total number of samples totaling 15 devices obtained from 3 Faculties and 7 official buildings at the University of Mataram, the percentage of 40% vulnerable to Deauthentication Attacks was obtained.

***Key words*: Wi-Fi, Vulnerable, Access Point, Denial of Service (DoS), Deauthentication Attack.**

I. PENDAHULUAN

Di era modern atau era millennial ini, keamanan jaringan merupakan suatu hal yang sangat penting dalam sebuah perangkat yang digunakan untuk menyediakan berbagai macam layanan bagi para penggunanya salah satunya berupa layanan untuk melakukan akses ke jaringan internet. Dikarenakan saat ini tidak dapat dipungkiri bahwa hampir seluruh kegiatan manusia membutuhkan akses ke jaringan internet sebagai penunjang kehidupan mulai dari bekerja, mencari pekerjaan, berniaga hingga melakukan komunikasi antar sesama pun membutuhkan akses ke jaringan internet.

Jaringan Wi-Fi banyak tersedia melalui perangkat keras yang bernama *access point* dikarenakan perangkat *access point* berfungsi sebagai penyebar sinyal internet kepada perangkat yang terhubung dan umumnya *access point* akan disambungkan dengan perangkat keras seperti router, hub atau switch melalui kabel ethernet agar dapat memancarkan sinyal [1].

Denial of Service (DoS) merupakan sebuah usaha (dalam bentuk serangan) untuk melumpuhkan suatu sistem (jaringan komputer) yang dijadikan target sehingga sistem tersebut tidak dapat menyediakan layanannya atau tingkat pelayanannya menurun dengan drastis. Cara untuk melumpuhkan dapat bermacam-macam dan akibatnya pun dapat beragam diantaranya yaitu sistem yang diserang dapat menjadi hang, crash, tidak berfungsi, atau turun kinerjanya (beban CPU tinggi) [3]. Terdapat berbagai jenis atau tipe serangan dari *Denial of Service* (DoS) dan salah satu jenis atau tipe serangan dengan dampak yang cukup mengganggu kenyamanan bagi para pengguna jaringan Wi-Fi ketika dalam keadaan menggunakan suatu jaringan Wi-Fi yaitu *Deauthentication Attack*.

Deauthentication Attack merupakan metode penyerangan jaringan komunikasi yang dapat dikategorikan sebagai salah satu jenis atau tipe dari serangan *Denial of Service* (DoS) dengan dampak yang dapat menyebabkan kelumpuhan komunikasi pada sebuah perangkat pemancar sinyal sehingga dapat menyebabkan terputusnya koneksi internet pada sebuah perangkat yang sedang terhubung [4][5]. Terdapat beberapa cara untuk melakukan penyerangan metode *Deauthentication Attack* yaitu menggunakan software kismet, aircrack, airodump-ng, airplay-ng, fluxion, MDK3, dan menggunakan perantara alat IoT NodeMCU ESP8266, dalam setiap penggunaan software atau alat baik dalam bentuk software ataupun hardware memiliki kelebihan dan kekurangan tersendiri, untuk penggunaan alat (hardware) untuk melancarkan serangan yaitu alat IoT (Internet of Things) berupa NodeMCU ESP8266 sedikit berbeda karena alat IoT ini bertugas menjadi perantara untuk melakukan penyerangan ke jaringan Wi-Fi dengan cara melakukan skema pendekatan pada jaringan Wi-Fi yang akan dieksekusi [6].

Dengan adanya metode penyerangan *Deauthentication Attack* tidak menutup kemungkinan metode ini dapat dengan mudah digunakan untuk melakukan penyerangan pada *access point* yang menyediakan akses ke jaringan Wi-Fi sehingga menyebabkan ketidaknyamanan pengguna

dalam menggunakan jaringan Wi-Fi, serangan ini akan membanjiri *access point* target dengan Deauthentication packet sehingga mengacaukan layanan pada client (pengguna jaringan Wi-Fi) dan mengakibatkan pengguna terputus dari jaringan Wi-Fi yang sedang digunakan dan yang sudah terhubung sebelumnya, jika pengguna mencoba untuk menghubungkan kembali koneksinya dengan Wi-Fi yang telah terserang metode *Deauthentication Attack* maka koneksinya akan diputuskan kembali. Dampak ini pun akan dirasakan oleh penyedia jaringan Wi-Fi dikarenakan jika pada perangkat *access point* penyedia jaringan Wi-Fi menggunakan perangkat dengan jenis atau merk dan versi firmware yang digunakan tidak menggunakan versi terbaru yang aman dengan metode penyerangan *Deauthentication Attack* maka penyerangan akan dapat dilakukan secara terus menerus serta dampak yang diterima akan terus dialami. Hal ini dapat menyebabkan banyak keluhan dari pengguna yang koneksinya terputus dan dapat membahayakan keamanan lalu lintas data para pengguna jaringan Wi-Fi [7].

Metode *Deauthentication Attack* dapat dijadikan sebagai langkah awal terjadinya pencurian data-data penting pengguna jaringan Wi-Fi, hal ini dilakukan dengan memanfaatkan pemutusan koneksi jaringan Wi-Fi pengguna melalui serangan *Deauthentication Attack* kemudian mempersiapkan sebuah SSID Wi-Fi palsu yang dalam hal ini SSID Wi-Fi tersebut diberikan nama yang sama dengan SSID Wi-Fi yang telah terhubung sebelumnya dengan tujuan untuk mengelabui pengguna jaringan Wi-Fi, pengguna yang terhubung akan diarahkan menuju sebuah laman login palsu (fake captive portal), jika pengguna tidak teliti pada saat diarahkan menuju laman login palsu maka pengguna akan mengisi data-data penting seperti e-mail, password, hingga username akun pengguna sehingga data-data tersebut secara otomatis akan didapatkan oleh penyerang tersebut dan tentunya akun pengguna tersebut dengan mudah disalahgunakan [8].

II. TINJAUAN PUSTAKA

Pada penelitian [9] mendemonstrasikan implementasi dari salah satu jenis dari serangan *Denial of Service* (DoS) yaitu serangan *Deauthentication Attack* pada jaringan wireless di frekuensi jaringan 802.11i menggunakan alat aireplay-ng dan MDK3 di sistem operasi KaliLinux 2018 [9]. Dalam hal ini kesamaan terletak pada metode penyerangan yang digunakan yaitu *Deauthentication Attack* namun terdapat beberapa perbedaan yang terletak pada penggunaan alat yang digunakan yang dimana penelitian yang diajukan menggunakan alat berbasis IoT yaitu nodemcu ESP8266, frekuensi jaringan yang diujikan pada penilitian yang diajukan tidak menghiraukan jenis frekuensi yang ada pada frekuensi jaringan 802.11 serta perangkat yang diujikan berupa *access point*, dan sistem operasi yang digunakan untuk melakukan skema penyerangan yaitu sistem operasi windows.

Pada penelitian [10] difokuskan pada pendeteksian dari salah satu jenis serangan *Denial of Service* (DoS) yaitu serangan *Deauthentication Attack* menggunakan *access point* sebagai perangkat untuk melakukan pendeteksian serangan *Deauthentication Attack* kemudian menggunakan algoritma MAC SDP DoS yang kemudian dimodifikasi menjadi algoritma MAC SDP DoS versi modifikasi [10]. Dalam hal ini kesamaan terletak pada metode penyerangan yang digunakan yaitu *Deauthentication Attack* namun terdapat beberapa perbedaan yang terletak pada fokus penelitian yang dimana penelitian yang diajukan difokuskan untuk mencari data persentase jumlah Wi-Fi *access point* yang vulnerable dan tidak vulnerable terhadap serangan DoS tersebut dan tidak untuk melakukan pendeteksian serangan, kemudian pada penggunaan alat yang digunakan yang dimana penelitian ini menggunakan *access point* sebagai alat untuk melakukan pendeteksian sedangkan penelitian yang diajukan menggunakan alat berbasis IoT yaitu nodemcu ESP8266 serta sistem operasi dan software yang digunakan untuk melakukan skema penyerangan.

Pada penelitian [11] membahas tentang bagaimana sebuah alat berbasis IoT berupa nodemcu ESP8266 V3 Lolin yang diprogramkan menggunakan program Arduino sebagai software pengujian dengan tujuan untuk membuktikan bahwa alat tersebut dapat melakukan scanning dapat mendeteksi (melakukan scanning) pada jaringan Wi-Fi yang tersedia disekitar alat tersebut diaktifkan dan melakukan percobaan untuk melakukan penyerangan pada jaringan ¬Wi-Fi tersebut menggunakan skema serangan *Denial of Service* (DoS) dengan jenis serangan *Deauthentication Attack* [11]. Pada penelitian ini terdapat beberapa kesamaan dengan penelitian yang diajukan yang terletak pada metode penyerangan yang digunakan yaitu *Deauthentication Attack* dengan tools atau alat berupa nodemcu ESP8266 V3 Lolin, namun dengan perbedaan pada penelitian yang diajukan terkait tujuan yaitu difokuskan untuk mencari data persentase jumlah Wi-Fi *access point* yang vulnerable dan tidak vulnerable terhadap serangan DoS tersebut serta mencari tahu penyebab dari suatu jaringan Wi-Fi pada *access point* tersebut dapat dikatakan vulnerable dan tidak vulnerable terhadap metode *Deauthentication Attack*.

Berdasarkan tinjauan pustaka yang telah dilakukan, relevansi antara penelitian terkait secara keseluruhan dengan penelitian yang diajukan adalah memiliki kesamaan dalam metode yang digunakan yaitu salah satu dari jenis serangan *Denial of Service* (DoS) berupa *Deauthentication Attack*, target yang diujikan berupa jaringan ¬Wi-Fi namun dengan perbedaan tujuan atau fokus yang ingin dihasilkan yang dimana pada penelitian yang diajukan difokuskan untuk mencari data persentase jumlah Wi-Fi *access point* yang vulnerable dan tidak vulnerable terhadap serangan DoS tersebut serta mencari tahu penyebab dari suatu jaringan Wi-Fi pada *access point* tersebut dapat dikatakan vulnerable dan tidak vulnerable terhadap metode *Deauthentication Attack*.

III. METODOLOGI

A. Analisis Alat dan Bahan Penelitian

Analisis alat dan bahan penelitian dilakukan untuk mengetahui alat dan bahan yang dibutuhkan berdasarkan perangkat keras dan perangkat lunak yang kemudian akan digunakan untuk penelitian, Adapun alat dan bahan yang dibutuhkan sebagai berikut:

A.1 Alat

1) Perangkat Keras

TABEL I. PERANGKAT KERAS

No	Nama Perangkat	Spesifikasi
1.	Laptop	- Windows OS - 8 GB RAM - Ryzen 3 Processor - 256 SSD
2.	NodeMCU ESP8266 V3 Lolin	

2) Perangkat Lunak

TABEL II. PERANGKAT LUNAK

No	Nama Perangkat
1.	Windows OS (Windows 11)
2.	Google Chrome
3.	Screen Recorder
4.	SpacehuhnTech ESP8266 Deauther Version 2

A.2 Bahan

Literatur yang dilakukan berkaitan dengan salah satu jenis atau tipe serangan dari *Denial of Service* (DoS) yaitu *Deauthentication Attack*, jaringan *wireless fidelity* (Wi-Fi), *access point* sebagai media untuk memperluas jaringan Wi-Fi.

B. Menentukan Lokasi Penelitian

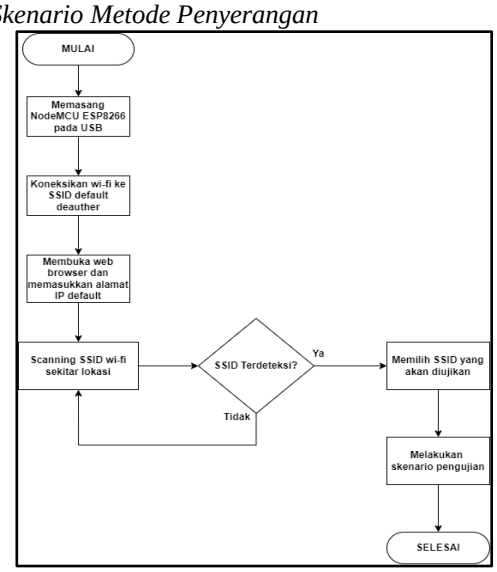
Pada tahapan ini dilakukan penentuan lokasi penelitian dengan tujuan untuk membatasi area atau lokasi yang akan diujikan dan memudahkan untuk perhitungan persentase jumlah *vulnerable* dan tidak *vulnerable* suatu jaringan Wi-Fi pada *access point* disetiap area atau lokasi, adapun penelitian dilakukan di lingkungan kampus utama (kampus 1) Universitas Mataram dengan lingkup yaitu beberapa fakultas dari seluruh fakultas yang terdapat pada kampus utama sebagai *sample* yang meliputi gedung belajar mengajar dan gedung akademik pada setiap fakultas dan pada setiap gedung atau bangunan resmi pihak Universitas Mataram yang memiliki jaringan Wi-Fi yang meliputi gedung PKM, gedung Rumah Sakit Unram, gedung LPMPP, gedung BPU (Badan Pengelola Usaha), Rusunawa Universitas Mataram, gedung LPPM, gedung Perpustakaan dan gedung Pusat Bahasa.

C. Instalasi Perangkat Lunak

Pada tahapan ini dilakukan instalasi perangkat lunak dengan menggunakan *software NodeMCU-flasher* sebagai langkah awal untuk melakukan *flashing* (install ulang) pada *NodeMCU ESP8266*, selanjutnya melakukan instalasi *software SpacehuhnTech ESP8266 Deauther Version* 2 dengan format bin sebagai *software* untuk melakukan uji coba metode penyerangan *Deauthentication Attack.*

D. Pengujian

D.1 Skenario Metode Penyerangan



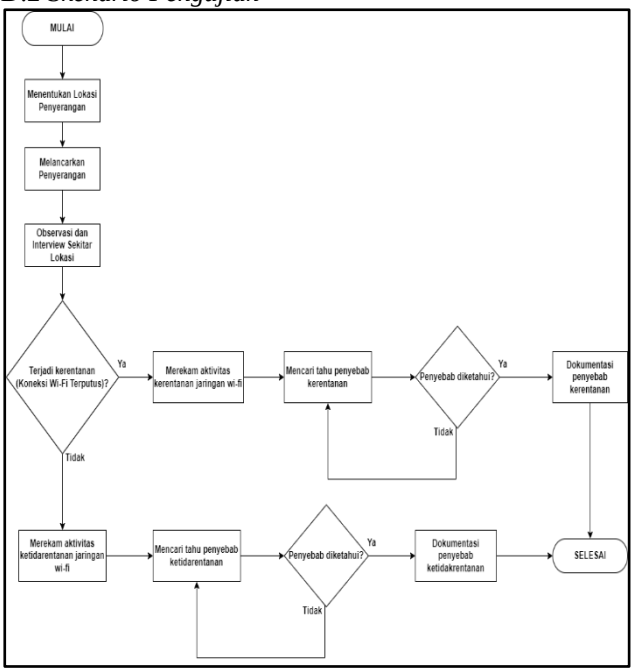
Gambar 1. Skenario Penyerangan.

Pada tahap skenario penyerangan akan dilakukan pengujian metode penyerangan menggunakan metode *Deauthentication Attack* terhadap *access point* yang memiliki jaringan Wi-Fi. Pada tahapan ini bertujuan untuk mengetahui cara penggunaan metode *Deauthentication Attack.* Adapun tahap skenario penyerangan adalah sebagai berikut:

1) Langkah pertama dimulai dengan memasang alat IoT *NodeMCU ESP8266* pada USB, USB yang digunakan untuk menghubungkan *NodeMCU ESP8266* adalah USB tipe *micro* atau *micro* USB dikarenakan pada *NodeMCU ESP8266* menggunakan *port micro* USB, USB dapat dipasangkan pada perangkat laptop ataupun menggunakan *powerbank* (alat penyimpan daya) untuk mengaktifkan *NodeMCU ESP8266.*
2) Langkah kedua melakukan koneksi Wi-Fi laptop ke SSID *default* alat *Deauther*, nama SSID dan *password* merupakan *default* yang secara otomatis terintegrasi dengan *software SpacehuhnTech ESP8266 Deauther Version* 2 yang telah diinstal pada alat *NodeMCU ESP8266*, SSID *default* dinamakan "pwned" dengan password *default* "deauther".
3) Langkah selanjutnya membuka *web browser* dan memasukkan alamt IP *default*, adapun *web browser* yang digunakan adalah *google chrome* dan alamat IP *default* yang secara otomatis terintegrasi setelah menginstall *software Deauther* adalah "192.168.4.1".
4) Langkah selanjutnya melakukan *scanning* SSID Wi-Fi yang terdapat disekitar lokasi pengujian, *scanning* Wi-Fi dapat dilakukan dengan cara menekan *scan apps* pada *web browser.*

5) Jika SSID Wi-Fi disekitar lokasi tidak terdeteksi, maka akan dilakukan *scanning* ulang SSID hingga mendapatkan SSID Wi-Fi disekitar lokasi.
6) Langkah selanjutnya memilih SSID Wi-Fi yang akan diujikan sesuai dengan lokasi yang ditentukan, *Deauther* dapat melakukan penyerangan lebih dari satu jaringan Wi-Fi yang terdeteksi dalam waktu yang bersamaan namun kinerja penyerangan dari *Deauther* ini tidak maksimal jika dilakukan dalam waktu yang bersamaan maka untuk mendapatkan hasil yang maksimal dilakukan dengan memilih satu persatu SSID yang terdeteksi oleh *Deauther*.
7) Langkah terakhir adalah melakukan skenario pengujian.

D.2 Skenario Pengujian



Gambar 2. Skenario Pengujian

Pada tahap skenario pengujian akan dilakukan langkah-langkah dalam pengujian metode menggunakan metode *Deauthentication Attack* terhadap *access point* yang memiliki jaringan Wi-Fi. Pada tahapan ini bertujuan untuk mengetahui dan mengumpulkan data apakah suatu jaringan Wi-Fi pada *access point* dapat dikatakan *vulnerable* dan tidak *vulnerable* terhadap metode *Deauthentication Attack*. Adapun tahap skenario pengujiannya adalah sebagai berikut:

1) Langkah pertama dimulai dengan menentukan lokasi penyerangan.
2) Langkah kedua melancarkan serangan menggunakan metode *Deauthentication Attack*, langkah-langkah cara melancarkan penyerangan dilakukan sesuai dengan skenario metode penyerangan.
3) Langkah selanjutnya melakukan observasi dan *interview* sekitar, observasi dilakukan untuk memantau keadaan sekitar apakah terdapat *user* yang sedang menggunakan jaringan Wi-Fi pada *access point* yang disediakan dilokasi tersebut, *interview* sekitar lokasi bertujuan untuk melakukan validasi dengan cara memberikan pertanyaan ke beberapa *user* sebagai *sample* yang sedang menggunakan koneksi jaringan Wi-Fi dilokasi tersebut apakah koneksi jaringan Wi-Fi yang sedang digunakan terputus atau tidak.
4) Berdasarkan langkah sebelumnya, jika *user* jaringan Wi-Fi tersebut memberikan jawaban bahwa koneksi yang digunakan terputus maka dapat dikatakan jaringan Wi-Fi pada *access point* tersebut *vulnerable* terhadap metode yang digunakan, sedangkan jika *user* memberikan jawaban bahwa koneksi yang digunakan tidak terputus maka dapat dikatakan jaringan Wi-Fi pada *access point* tersebut tidak *vulnerable* terhadap metode yang digunakan.
5) Kemudian melakukan perekaman aktivitas terputus atau tidaknya koneksi pada jaringan Wi-Fi menggunakan *software screen recorder* atau melakukan perekaman secara langsung menggunakan *handphone*, perekaman dilakukan pada laptop dan perangkat yang digunakan oleh *user*.
6) Langkah selanjutnya mencari tahu penyebab kerentanan dan ketidakrentanan jaringan Wi-Fi pada *access point* dilokasi yang telah ditentukan, penyebab kerentanan dapat diketahui dari segi *hardware* atau perangkat *access point* yang digunakan dan *software* yang telah ter-*install* pada perangkat *access point* tersebut.
7) Jika penyebab dari kerentanan dan ketidakrentanan jaringan Wi-Fi pada *access point* yang diujikan telah diketahui, maka dilakukan dokumentasi penyebab kerentanan dan ketidakrentanan tersebut, dokumentasi berupa vidio aktivitas pengujian kerentanan dan ketidakrentanan terhadap metode *Deauthentication Attack* serta dokumentasi laporan.

Adapun hasil dari skema pengujian yang telah dilakukan akan digunakan perhitungan jumlah total persentase dan tabel hasil pengujian dengan rincian sebagai berikut:

1) Perhitungan Jumlah Total Persentase

Adapun perhitungan persentase jumlah perangkat yang dikatakan *vulnerable* (rentan) dan tidak *vulnerable*:

- Perhitungan persentase perangkat *vulnerable*

$$\frac{Jumlah\ Perangkat\ Vulnerable}{Jumlah\ Perangkat\ yang\ diujikan} \times 100\% = \ldots \quad (1)$$

- Perhitungan persentase perangkat tidak *vulnerable*

$$\frac{Jumlah\ Perangkat\ Tidak\ Vulnerable}{Jumlah\ Perangkat\ yang\ diujikan} \times 100\% = \ldots \quad (2)$$

E. Pencatatan Status Vulnerability

TABEL III. HASIL PENCATATAN

No	**Lokasi Perangkat (Fakultas/ Jurusan/ Gedung)**	**Nama SSID Wi-Fi**	**Jenis /Merk *Hardware* (*access point*)**	**Versi *Firmware***	**Status *Vulnerability* (*Deauthentication*)**

Pencatatan status *vulnerability* dimaksudkan untuk memberikan status pada perangkat *access point* yang telah dilakukan penyerangan berdasarkan jenis/merk *hardware* (*access point*) dan versi *firmware* sebagai faktor penyebab *vulnerability* apakah perangkat yang diujikan memiliki keamanan terhadap metode *Deauthentication Attack* atau tidak serta mendapatkan data jumlah perangkat yang *vulnerable* atau tidak terhadap metode *deauthenticataion attack*, untuk melakukan pengisian pada kolom status *vulnerability* perlu dilakukan analisis terhadap aktivitas penyerangan yang dilakukan terhadap jaringan Wi-Fi pada *access point*, link vidio aktivitas penyerangan akan didokumentasikan melalui media *google drive* untuk mempermudah analisis aktivitas penyerangan melalui perekaman layar agar dapat mengetahui jaringan Wi-Fi yang diujikan *vulnerable* atau tidak *vulnerable* menggunakan metode *Deauthentication Attack.*

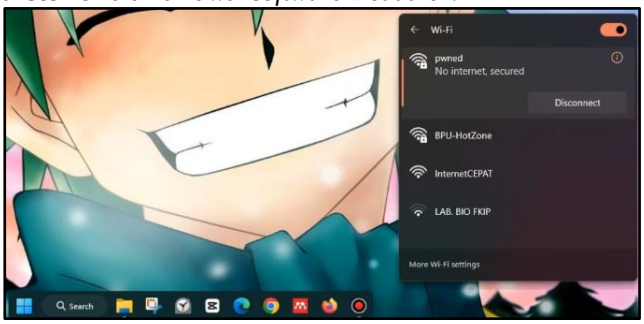
IV. HASIL DAN PEMBAHASAN

A. Realisasi Skema Penyerangan Deauthentication Attack

Pada sub bab ini merupakan realisasi penyerangan yang dilakukan dengan menggunakan metode *Deauthentication Attack*, realisasi skema penyerangan disesuaikan berdasarkan pada bab sebelumnya, realisasi ini akan membahas bagaimana proses metode *Deauthentication Attack* dilakukan hingga akibat dari serangan ini yaitu terputusnya koneksi pada sebuah perangkat yang sedang terhubung pada jaringan Wi-Fi. Adapun tahapan – tahapan skema penyerangan *Deauthentication Attack* sebagai berikut:

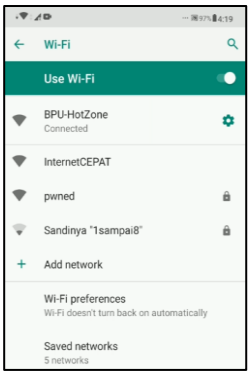
Gambar 3. Koneksi Laptop ke NodeMCU ESP8266

Pada Gambar 3 merupakan proses untuk menghubungkan alat *Deauther* dari perangkat laptop agar dapat melakukan akses ke halaman awal *software Deauther*.



Gambar 4. Koneksi ke SSID Default Deauther

Pada Gambar 4 merupakan proses untuk menghubungkan perangkat laptop ke SSID Wi-Fi *Deauther* setelah dilakukannya menghubungkan NodeMCU ESP8266 yang telah ter-*install software Deauther* oleh *SpacehuhnTech ESP8266 Deauther Version* 2 dari perangkat laptop menggunakan *port micro* USB.

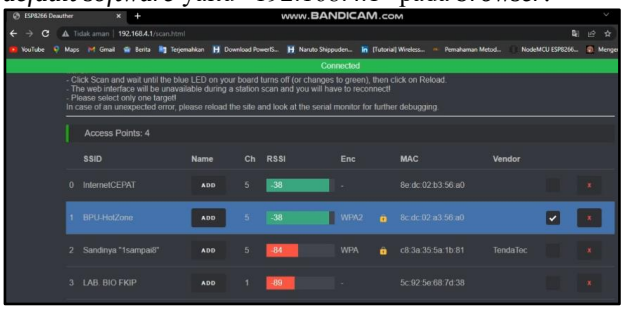


Gambar 5. Status Koneksi Wi-Fi Pada Perangkat Target

Pada Gambar 5 merupakan status koneksi pada perangkat target dengan status *connected* atau terkoneksi.

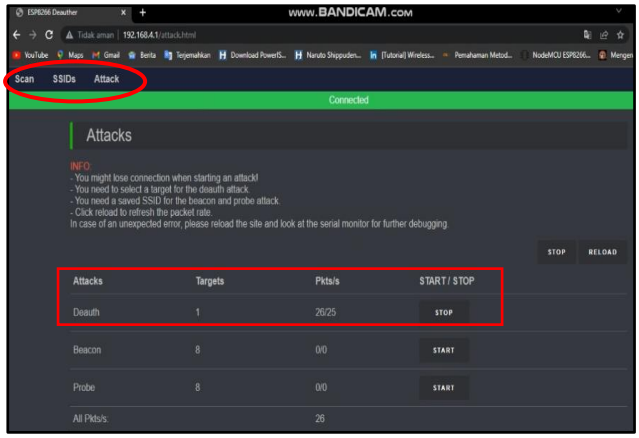
Gambar 6. User Interface Software Deauther Versi 2

Pada Gambar 6 merupakan tampilan *user interface software Deauther* versi 2 oleh *SpacehuhnTech*, halaman ini dapat diakses dengan cara memasukkan *IP address default software* yaitu “192.168.4.1” pada *browser*.



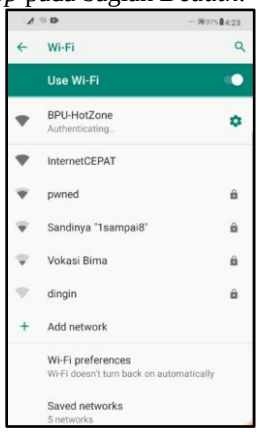
Gambar 7. *Scanning* SSID Wi-Fi Target

Setelah melewati halaman awal sebelumnya, kemudian memasuki tahapan berikutnya yaitu pada Gambar 7 merupakan proses dilakukannya *scanning* SSID Wi-Fi yang akan dilakukan penyerangan, pada proses ini menampilkan kekuatan sinyal jaringan Wi-Fi sesuai dengan jarak alat *Deauther* yang telah terpasang, pada proses ini pemilihan target penyerangan dilakukan hanya 1 jaringan Wi-Fi untuk memaksimalkan kinerja penyerangan.



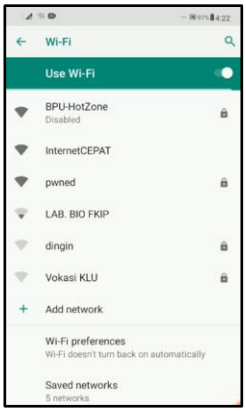
Gambar 8. Melancarkan Penyerangan

Setelah dilakukannya *scanning* SSID Wi-Fi yang akan dilakukan penyerangan, selanjutnya melakukan penyerangan dengan cara menekan *Attack* pada menu bagian atas halaman yang kemudian dilanjutkan pada Gambar 8 yang merupakan proses dilakukannya penyerangan dengan cara menekan *start* pada bagian *Deauth*, pada proses ini *Deauther* mulai mengirimkan paket-paket berupa *Deauthentication Frame* ke perangkat jaringan Wi-Fi yang ditargetkan, akibat dari proses ini akan dikatakan berhasil apabila perangkat *target* mengalami terputusnya koneksi jaringan Wi-Fi, sedangkan jika keamanan jaringan pada perangkat dapat menangani serangan ini maka pada perangkat target tidak akan terjadi apapun terhadap koneksi jaringan Wi-Fi perangkat tersebut. Proses ini dapat dihentikan dengan cara menekan *stop* pada bagian *Deauth*.



Gambar 9. Respon Wi-Fi Target

Gambar 9 merupakan respon pada perangkat target yang sedang terhubung pada jaringan Wi-Fi, pada Gambar 9 memperlihatkan perangkat target mencoba untuk menghubungkan Kembali ke jaringan Wi-Fi yang telah terputus oleh *Deauther*.



Gambar 10. Respon Hasil Akhir Wi-Fi Target

Gambar 10 meurpakan respon akhir setelah perangkat target mencoba untuk menghubungkan kembali pada jaringan Wi-Fi yang telah terhubung sebelumnya namun perangkat tersebut tidak dapat menghubungkan kembali pada jaringan Wi-Fi sehingga dapat dikatakan perangkat jaringan Wi-Fi tersebut rentan terhadap *Deauthentication Attack*.

B. Analisis Hasil Serangan Deauthentication Attack

Berikut merupakan tabel hasil pencatatan status *vulnerability* setelah dilakukan penyerangan menggunakan *Deauthentication Attack*:

TABEL IV. HASIL PENCATATAN STATUS *VULNERABILITY*

No.	**Lokasi Perangkat (Fakultas /Jurusan/ Gedung)**	**Nama SSID Wi-Fi**	**Jenis /Merk *Hardware* (*access point*)**	**Versi *Firmware***	**Status**
1.	UPT. Pusat Bahasa	@unram.ac.id	*Ruijie* RG-AP820-L	AP_RGOS 11.9(4)B1	*Non-Vulnerable* (Tidak Rentan)
2.	UPT. Perpustakaan	1. @unram.ac.id 2. @unram.ac.id 3. @KTU.NET 4. @TU.NET 5. R.Pengadaan	*Ruijie* RG-AP720-L *Ruijie* RG-AP820-L TP link TL-WR840N TP Link WR720N 150 mbps TP link-TL-WR840N	AP_RGOS 11.1(9)B1P19 AP_RGOS 11.9(4)B1 Versi 3.16.9 Versi 1.0.0 Versi 3.16.9	*Non-vulnerable* (Tidak Rentan) *Non-vulnerable* (Tidak Rentan) *Vulnerable* (Rentan) *Vulnerable* (Rentan) *Vulnerable* (Rentan)
3.	UPT. BPU (Badan Pengelola Usaha)	BPU-HotZone	ZTE F609	V7.0.10P1T11	*Vulnerable* (Rentan)

4.	Gedung LPMPP	@unram.ac.id	*Ruijie* RG-AP820-L	AP_RGOS 11.9(4)B1	*Non-vulnerable* (Tidak Rentan)
5.	Gedung PKM	@unram.ac.id	*Ruijie* RG-AP820-L	AP_RGOS 11.9(4)B1	*Non-vulnerable* (Tidak Rentan)
6.	Gedung LPPM	@unram.ac.id	*Ruijie* RG-AP820-L	AP_RGOS 11.9(4)B1	*Non-Vulnerable* (Tidak Rentan)
7.	Gedung Rumah Sakit UNRAM	1. PaSya 2. R.SERVER	*Ruijie* EW300-PRO Totolink N200RE	ReyeeOS 1.59.1417 V3.4.0-B20190813	*Vulnerable* (Rentan) *Vulnerable* (Rentan)
8.	Fakultas Mipa	@Mipa@unram.ac.id	*Ruijie* RG-AP720-L	AP_RGOS 11.1(9)B1P19	*Non-Vulnerable* (Tidak Rentan)
9.	Fakultas Teknik	@unram.ac.id	*Ruijie* RG-AP820-L	AP_RGOS 11.9(4)B1	*Non-vulnerable* (Tidak Rentan)
10.	Fakultas Pertanian	@unram.ac.id	*Ruijie* RG-AP820-L	AP_RGOS 11.9(4)B1	*Non-vulnerable* (Tidak Rentan)

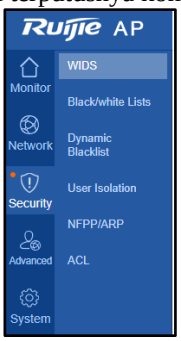
1) Perangkat *vulnerable* (rentan) ditemukan di beberapa titik lokasi berdasarkan data berupa vidio aktivitas perakaman layar yaitu:
   - UPT. Perpustakaan, Jumlah sampel yang telah diambil yaitu berjumlah (5 perangkat) dikarenakan jumlah perangkat access point yang cukup banyak serta berlokasi hampir di seluruh ruangan pada gedung UPT. Perpustakaan, berdasarkan total sampel yang diambil ditemukan 3 perangkat yang tergolong rentan (vulnerable) yaitu perangkat dengan jenis atau merk (TP link TL-WR840N, TP Link WR720N 150 mbps, TP link-TL-WR840N) dengan nama SSID wi-fi (@KTU.NET, @TU.NET, R.Pengadaan) dengan tahun produksi pada tahun 2012 untuk TP link WR720N 150 mbps dan 2013 untuk TP link WR840N.
   - UPT. BPU (Badan Pengelola Usaha), Jumlah sampel yang telah diambil yaitu berjumlah (1 perangkat) dikarenakan jumlah perangkat access point yang digunakan hanya satu perangkat untuk seluruh area lokasi gedung UPT.BPU, perangkat yang dijadikan sampel adalah perangkat dengan jenis atau merk (ZTE F609) dengan nama SSID wi-fi (BPU-HotZone) dengan tahun produksi pada tahun 2013.
   - Gedung Rumah Sakit UNRAM, Jumlah sampel yang telah diambil yaitu berjumlah (2 perangkat) dikarenakan jumlah perangkat access point yang cukup banyak serta berlokasi hampir di seluruh ruangan pada gedung Rumah Sakit UNRAM, berdasarkan total sampel yang diambil, keseluruhan sampel tersebut merupakan perangkat yang tergolong rentan (vulnerable) yaitu perangkat dengan jenis atau merk (Ruijie EW300-PRO, Totolink N200RE) dengan nama SSID wi-fi (PaSya, R.SERVER) dengan tahun produksi pada tahun 2022 untuk Ruijie EW300-PRO dan 2015 Totolink N200RE.

2) Perangkat *non vulnerable* (tidak rentan) ditemukan di beberapa titik lokasi berdasarkan data berupa vidio aktivitas perakaman layar yaitu:
   - UPT. Pusat Bahasa, Jumlah sampel yang telah diambil yaitu berjumlah (1 perangkat) dikarenakan jumlah perangkat access point yang cukup banyak serta berlokasi hampir di seluruh ruangan pada gedung UPT. Pusat Bahasa serta perangkat access point yang digunakan hanya satu jenis perangkat untuk seluruh area lokasi gedung UPT. Pusat Bahasa, perangkat yang dijadikan sampel adalah perangkat dengan jenis atau merk (Ruijie RG-AP820-L) dengan nama SSID wi-fi (@unram.ac.id) dengan tahun produksi pada tahun 2016.
   - UPT. Perpustakaan, Jumlah sampel yang telah diambil yaitu berjumlah (5 perangkat) dikarenakan jumlah perangkat access point yang cukup banyak serta berlokasi hampir di seluruh ruangan pada gedung UPT. Perpustakaan, berdasarkan total sampel yang diambil ditemukan 2 perangkat yang tergolong tidak rentan (non-vulnerable) yaitu perangkat dengan jenis atau merk (Ruijie RG AP720-L, Ruijie RG-AP820-L) dengan nama SSID wi-fi (@unram.ac.id) dengan tahun produksi pada tahun 2016.
   - Gedung LPPM, Jumlah sampel yang telah diambil yaitu berjumlah (1 perangkat) dikarenakan jumlah perangkat access point yang cukup banyak dan berlokasi hampir di seluruh ruangan pada gedung LPPM serta perangkat access point yang digunakan hanya satu jenis perangkat untuk seluruh area lokasi gedung LPPM, perangkat yang dijadikan sampel adalah perangkat dengan jenis atau merk (Ruijie RG-AP820-L) dengan nama SSID wi-fi (@unram.ac.id) dengan tahun produksi pada tahun 2016.
   - Gedung LPMPP, Jumlah sampel yang telah diambil yaitu berjumlah (1 perangkat) dikarenakan jumlah perangkat access point yang cukup banyak serta berlokasi hampir di seluruh ruangan pada gedung LPMPP serta perangkat access point yang digunakan hanya satu jenis perangkat untuk seluruh area lokasi gedung LPMPP, perangkat yang dijadikan sampel adalah perangkat dengan jenis atau merk (Ruijie RG-AP820-L) dengan nama SSID wi-fi (@unram.ac.id) dengan tahun produksi pada tahun 2016.

- Gedung PKM, Jumlah sampel yang telah diambil yaitu berjumlah (1 perangkat) dikarenakan jumlah perangkat access point yang cukup banyak serta berlokasi hampir di seluruh ruangan pada gedung PKM serta perangkat access point yang digunakan hanya satu jenis perangkat untuk seluruh area lokasi gedung PKM, perangkat yang dijadikan sampel adalah perangkat dengan jenis atau merk (Ruijie RG-AP820-L) dengan nama SSID wi-fi (@unram.ac.id) dengan tahun produksi pada tahun 2016.
- Fakultas Teknik, Jumlah sampel yang telah diambil yaitu berjumlah (1 perangkat) dikarenakan jumlah perangkat access point yang cukup banyak serta berlokasi hampir di seluruh ruangan pada gedung Fakultas Teknik serta perangkat access point yang digunakan hanya satu jenis perangkat untuk seluruh area lokasi gedung Fakultas Teknik, perangkat yang dijadikan sampel adalah perangkat dengan jenis atau merk (Ruijie RG-AP820-L) dengan nama SSID wi-fi (@unram.ac.id) dengan tahun produksi pada tahun 2016.
- Fakultas Pertanian, Jumlah sampel yang telah diambil yaitu berjumlah (1 perangkat) dikarenakan jumlah perangkat access point yang cukup banyak serta berlokasi hampir di seluruh ruangan pada gedung Fakultas Pertanian serta perangkat access point yang digunakan hanya satu jenis perangkat untuk seluruh area lokasi gedung Fakultas Pertanian, perangkat yang dijadikan sampel adalah perangkat dengan jenis atau merk (Ruijie RG-AP820-L) dengan nama SSID wi-fi (@unram.ac.id) dengan tahun produksi pada tahun 2016.
- Fakultas MIPA (Matematika dan Ilmu Pengetahuan), Jumlah sampel yang telah diambil yaitu berjumlah (1 perangkat) dikarenakan jumlah perangkat access point yang cukup banyak serta berlokasi hampir di seluruh ruangan pada gedung Fakultas MIPA, berdasarkan sampel yang diambil yaitu perangkat dengan jenis atau merk (Ruijie RG-AP820-L) dengan nama SSID wi-fi (@unram.ac.id) dengan tahun produksi pada tahun 2016.

Berdasarkan tabel hasil pencatatan penyerangan menggunakan metode deauthentication attack, kerentanan terjadi diakibatkan beberapa lokasi menggunakan perangkat yang tergolong pada perangkat dengan jenis atau merk lama serta masih menggunakan versi firmware default perangkat sehingga mengakibatkan terputusnya koneksi pengguna wi-fi yang dapat dilihat pada data berupa vidio aktivitas perakaman layar.

Sedangkan ketidakrentanan (non-vulnerable) terjadi karena jenis atau merk perangkat serta firmware yang digunakan menggunakan versi baru dengan teknologi yang lebih mumpuni sehingga memungkinkan perangkat tersebut dapat menahan serangan dari metode deuthentication attack yang dapat dilihat pada data berupa vidio aktivitas perakaman layar, pada perangkat yang diujikan tidak terjadi terputusnya koneksi pengguna wi-fi.



Gambar 11 Fitur firmware pada sampel Ruijie RG-AP720-L

Pada Gambar 11 merupakan salah satu contoh perangkat yang memiliki fitur-fitur dengan teknologi yang baik dari segi firmware dengan memiliki fitur-fitur untuk menahan serangan deauthentication attack pada perangkat, Berbeda dengan perangkat non-vulnerable (Ruijie RG-AP820-L) yang memiliki fitur yang sama dengan Ruijie RG-AP720-L yaitu black/white lists, dynamic blacklist dan user isolation yang memiliki fungsi untuk meminimlisasi deauthentication attack, namun Rujie RG-AP720-L memiliki salah satu fitur yang tidak dimiliki pada perangkat non-vulnerable (Ruijie RG-AP820-L) yang terdapat pada konfigurasi perangkat ini adalah Wireless Intrusion Detection System (WIDS). WIDS bertujuan untuk mendeteksi aktivitas yang mencurigakan atau serangan pada jaringan Wi-Fi dan memberikan pemberitahuan kepada administrator yang kemudian administrator dapat mengambil tindakan untuk mengatasi hal tersebut. Fitur ini mendeteksi aktivitas jaringan dengan mengidentifikasi pola mencurigakan. Pola yang mencurigakan dapat mengindikasikan adanya serangan pada jaringan Wi-Fi, termasuk serangan deauthentication [22].

Dalam hal ini tahun produksi suatu perangkat dapat diperhitungkan sebelum dilakukannya pembelian hingga pemasangan karena pada umumnya semakin baru tahun keluaran perangkat maka teknologi dari segi hardware dan firmware yang digunakan tentunya menggunakan versi baru sehingga memungkinkan perangkat tersebut untuk mengabaikan berbagi serangan yang dapat terjadi sewaktu-waktu.

Minimalisasi dampak dari metode Deuthentication Attack dapat dilakukan dengan melakukan pergantian perangkat access point dengan cara memperhatikan jenis atau merk serta tahun keluaran perangkat yang akan dijadikan sebagai access point wi-fi, hal ini dapat dilakukan dengan mencari informasi terkait spesifikasi perangkat melalui laman resmi produsen perangkat. Cara lain yang dapat dilakukan yaitu dengan memperhatikan konfigurasi dari perangkat yang digunakan,

memperhatikan konfigurasi perangkat dapat dilakukan dengan cara melakukan akses pada firmware perangkat, kemudian melakukan pencarian informasi apakah perangkat tersebut memiliki fitur pada konfigurasi yang dapat mencegah terjadinya Deauthentication Attack serta dapat melakukan updating firmware pada perangkat jika versi firmware yang lebih baru pada perangkat tersebut memiliki fitur dengan teknologi yang dapat mencegah serangan.

C. Total Perhitungan Persentase Perangkat

Berdasarkan total jumlah perangkat yang telah diujikan yaitu berjumlah 15 perangkat *access point* dengan jumlah total perangkat *vulnerable* (rentan) berjumlah 6 dan *non-vulnerable* 9 maka didapatkan perhitungan:

1) Perhitungan persentase perangkat vulnerable

$$\frac{6}{15} \times 100\% = 40\ \% \quad (3)$$

2) Perhitungan persentase perangkat non vulnerable

$$\frac{9}{15} \times 100\% = 60\ \% \quad (4)$$

D. Klasifikasi Perangkat

Berdasarkan penyerangan menggunakan metode Deauthentication Attack yang telah dilakukan, ditemukan beberapa jenis atau merk perangkat access point yang digunakan di Universitas Mataram (kampus utama), klasifikasi bertujuan memberikan informasi terkait rekomendasi perangkat access point untuk meminimalisasi penyerangan.

TABEL V. *KLASIFIKASI PERANGKAT*

Disarankan (*non-vulnerable*):			
Nama Perangkat	**Jenis/ Merk**	**Versi Firmware**	**Gambar Perangkat**
Ruijie	Ruijie RG-AP820-L	AP_RGOS 11.9(4)B1	
Ruijie	Ruijie RG-AP720-L	AP_RGOS 11.1(9)B1P19	
Tidak Disarankan (*Vulnerable*):			
Nama Perangkat	**Jenis/Merk**	**Versi Firmware**	**Gambar Perangkat**
ZTE	ZTE F609	V7.0.10P1T11	
Ruijie	Ruijie EW300-PRO	ReyeeOS 1.59.1417	
Totolink	Totolink N200RE	V3.4.0-B20190813	
TP Link	TP Link WR720N 150 mbps	Versi 1.0.0	
TP link	TP link TL-WR840N	Versi 3.16.9	

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan penelitian dan pengujian yang telah dilaksanakan, dapat ditarik kesimpulan sebagai berikut:

1) Persentase jumlah jaringan wi-fi pada access point yang vulnerable (rentan) berjumlah 60% dan non-vulnerable (tidak rentan) 40% berdasarkan pada total jumlah sampel perangkat yang diujikan yaitu 15 perangkat (6 vulnerable dan 9 non-vulnerable) dari 3 Fakultas dan 7 bangunan resmi di Universitas Mataram.
2) Penyebab terjadinya vulnerability dikarenakan penggunaan perangkat access point yang masih menggunakan jenis atau merk lama serta menggunakan firmware default perangkat, sedangkan ketidakrentanan (non-vulnerable) dikarenakan penggunaan perangkat access point menggunakan jenis atau merk baru serta menggunakan firmware dengan teknologi yang lebih mumpuni.
3) Minimalisasi dampak dari metode Deuthentication Attack dapat dilakukan dengan cara melakukan pergantian perangkat access point, memperhatikan jenis atau merk, tahun keluaran dan konfigurasi yang diaplikasikan pada perangkat yang digunakan serta melakukan updating firmware pada perangkat jika versi firmware yang lebih baru pada perangkat tersebut memiliki fitur dengan teknologi yang dapat mencegah serangan.

B. Saran

Sebagai upaya untuk mengembangkan hasil yang didapatkan dalam penelitian ini agar menjadi lebih baik, beberapa saran yang dapat diberikan adalah sebagai berikut:

1) Memperbanyak sampel perangkat yang akan diambil agar dapat menemukan lebih banyak perangkat yang vulnerable (rentan) dan non-vulnerable (tidak rentan) khususnya di lingkungan kampus utama Universitas Mataram.
2) Memperdalam analisis penyebab terjadinya vulnerabilty pada suatu perangkat jaringan Wi-Fi dari segi konfigurasi firmware hingga melakukan update firmware agar dapat meminimalisasi dari berbagi jenis serangan salah satunya *Deauthentication Attack*.

3) Pengadaan perangkat access point dengan teknologi yang lebih mumpuni perlu diperhatikan agar terhindar dari berbagai jenis serangan pada perangkat salah satunya Deauthentication Attack.
4) Untuk pengembangan lebih lanjut, penelitian terhadap penyerangan perangkat jaringan Wi-Fi dapat menggunakan lebih dari satu jenis metode penyerangan agar dapat mengetahui tingkat keamanan pada suatu perangkat.

REFERENCES

[1] Sugiyono, "Sistem Keamanan Jaringan Komputer Menggunakan Metode Watchguard Firebox Pada Pt Guna Karya Indonesia," Jurnal Cki On Spot, Vol. 9, No. 1, 2016.

[2] Indones. Secur. Incid. Response Team Internet Infrastruct, "Pusat Operasi Keamanan Siber Nasional Badan Siber Dan Sandi Negara Indonesia Cyber Security Monitoring Report 2019," 2022. Accessed: Nov. 13, 2022. [Online]. Available: Https://Bssn.Go.Id/Laporan-Tahunan-Monitoring-Keamanan-Siber-Tahun-2021/

[3] S. Nurwenda, B. Irawan, And Irzaman, "Analisis Kelakuan Denial-Of-Service Attack (Dos Attack) Pada Jaringan Komputer Dengan Pendekatan Pada Level Sekuritas," 2004.

[4] M. Rafita, "Analisis Metode Fluxion Menggunakan Wi-Fi Deauther Untuk Uji Keamanan Wpa2 Pada Perangkat Router Wireless Totolink N300rt," 2022.

[5] K. Yogi, "Analysis Of *Deauthentication Attack* On Ieee 802.11 Connectivity Based On Iot Technology Using External Penetration Test," 2020. Doi: 10.21512/Commit.V14i1.6337.

[6] A. D. Pangestu, F. Ardianto, And B. Alfaresi, "Sistem Monitoring Beban Listrik Berbasis Arduino Nodemcu Esp8266," Vol. 4, No. 1, 2019.

[7] Y. Ahmad, A. Faiz, G. Jafaruddin, And W. Eka, "Analisis Network Security Pada Layanan Wifi Indihome Terhadap Serangan *Denial of Service* (Dos)," 2022. Doi: Http://Dx.Doi.Org/10.30811/Litek.V19i1.2884.

[8] J. M. Lunodzo, A. Z. Agghey, F. K. Shubi, And D. N. Jema, "Fakeap Detector: An Android-Based Client-Side Application For Detecting Wi-Fi Hotspot Spoofing," Ieee Access, Vol. 10, Pp. 13611–13623, 2022, Doi: 10.1109/Access.2022.3146802.

[9] C. Kamani, D. Bhojani, R. Bhagyoday, V. Parmar, And D. Dave, "De-Authentication Attack On Wireless Network," 2019. [Online]. Available: Https://Kalilinuxtutorials.Com/Mdk3/

[10] S. Shweta And M. Meenakshi, "Detection And Prevention Of De-Authentication Attack In Real-Time Scenario," International Journal Of Innovative Technology And Exploring Engineering, Vol. 8, No. 10, Pp. 3324–3330, Aug. 2019, Doi: 10.35940/Ijitee.J1217.0881019.

[11] K. Afif, S. Agung, I. Yuda, And J. Didi, "Alat Pengacau Sinyal Wi-Fi Dengan Nodemcu (Board V.3 Lolin) Esp8266 Deauther Berbasis Microcontroller," Jurnal Ilmiah Wahana Pendidikan, Vol. 8, No. 10, Pp. 231–237, 2022, Doi: 10.5281/Zenodo.6791842.

[12] R. Permana, D. Ramadhani, And I. Lestari, "Proteksi Keamanan Jaringan Komputer Di Sekolah Menengah Kejuran Al-Madani Pontianak," 2019, Doi: Https://Doi.Org/10.23887/Ijnse.V3i1.22175.

[13] Y. Febrison And Haeruddin, "Analisa Dan Implementasi Wireless Extension Point Dengan Ssid (Service Set Identifier)," 2020, Doi: Http://Dx.Doi.Org/10.37253/Joint.V1i2.4309.

[14] I. Anugrah And R. H. Rahmanto, "Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone," 2017. Doi: 10.33558/Piksel.V5i2.271.

[15] T. Mahjabin, Y. Xiao, G. Sun, And W. Jiang, "A Survey Of Distributed Denial-Of-Service Attack, Prevention, And Mitigation Techniques," Int J Distrib Sens Netw, Vol. 13, No. 12, Dec. 2017, Doi: 10.1177/1550147717741463.

[16] A. P. Rasky, H. F. Imansyah, And F. W. T. Pontia, "Rancang Bangun *Access point* Menggunakan Empat Perangkat Nanostation2 Loco (Ns2l) Pada Outdoor Hotspot System," 2014.

[17] I. Catur And S. Dedi, "Analisis Perbandingan Kinerja Dan Kualitas Layanan Antara Firmware Default Dan Firmware Openwrt Pada *Access point* Tp-Link Mr3020," Yogyakarta, 2017. Doi: 10.1109/Access.2022.3146802.

[18] R. Karim, S. S. Sumendap, And F. V. I. A. Koagouw, "Pentingnya Penggunaan Jaringan Wi-Fi Dalam Memenuhi Kebutuhan Informasi Pemustaka Pada Kantor Perpustakaan Dan Kearsipan Daerah Kota Tidore Kepulauan," 2016.

[19] Riska, W. G. Prama, And Patrick, "Analisa Dan Implementasi Wireless Extension Point Dengan Ssid (Service Set Identifier)," 2017.

[20] S. Seneviratne, F. Jiang, M. Cunche, And A. Seneviratne, Ssids In The Wild: Extracting Semantic Information From Wifi Ssidsoctober 2015. 2016. Doi: 10.1109/Lcn.2015.7366361.

[21] P. Denisky, "[Tutorial] Wireless *Deauthentication Attack*," 2020. [Online]. Available:Https://Id.Linkedin.Com/Pulse/Tutorial-Wireless-Deauthentication-Attack-Denisky-Patricio (Accessed Jan. 04, 2023).

[22] P. Desi, S. Hero, Herlawati, "Wireless Intrusion Detection System Pada STMIK Bina Insani," 2018.