OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

Implementasi Peretasan Jaringan Menggunakan Alat ESP8266 Dengan Teknik *Penetration Testing* Metode *Deauther* Dan *Beacon* Pada *Wireless* Tenda F3

Andrian Fakhrizal[1*], Yudi Kurniawan[1]

[1]Fakultas Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Jl. Raya Puspiptek No. 46, Kel. Buaran, Kec. Serpong, Kota Tangerang Selatan. Banten 15310, Indonesia
Email: [1*]andrianfakhrizal03@gmail.com@email.com, [2]dosen00298@unpam.ac.id
(* : coressponding author)

Abstrak− Internet sangat penting dan telah menjadi kebutuhan penting masyarakat di seluruh dunia, terutama dalam situasi saat ini. Jaringan internet bisa dijadikan konsep dimana beberapa komputer dalam suatu Perguruan Tinggi dapat saling berkomunikasi dan dapat berbagi data serta informasi yang terhubung dengan koneksi dunia. Dosen, karyawan, maupun mahasiswa(user) suatu waktu mengeluh karena penggunaan internet sangat lambat jika sedang padat pengguna. Karena adanya penggunaan Bandwidth yang berlebihan dan kurang termanajemennya dengan baik pada traffic jaringan, sehingga merugikan user lain. (Prihantoro dkk, 2021). SMK YMIK pernah mengalami gangguan pada internet dan menggunakan router Tenda F3 lalu menjelaskan seperti Jaringan tiba tiba putus dan internet lambat tiba tiba. Menurut keterangan gangguan tersebut di sebabkan oleh mungkin dengan berusaha membobol kata sandi. Dari uraian latar belakang diatas, maka penulis mencoba untuk membuat suatu penelitian yang bermanfaat, peretasan ini menggunakan metode deauther dan beacon dalam peretasan jaringan wifi. Perancangan penelitian ini berbasis microcontroller, alat yang digunakan penulis adalah NodeMCU ESP8266 untuk target peretasannya menggunakan Tenda F3. Dalam metode penelitian untuk mendapatkan data dan informasi maka metode yang digunakan dalam proses pengumpulan data dari berbagai sumber yang di lakukan adalah Observasi, Wawancara dan Studi PustakaDengan metode Deauther dan Beacon, karena penggunaan metode tersebut untuk tujuan ilegal dan tidak etis. Namun, peneliti dapat memberikan informasi tentang hasil pengujian yang telah dilakukan terkait dengan metode ini. Penelitian telah dilakukan dengan menggunakan metode Deauther dan Beacon untuk menguji keamanan jaringan Wi-Fi. Hasilnya menunjukkan bahwa metode ini sangat efektif dalam meretas jaringan Wi-Fi yang tidak dienkripsi atau dilindungi dengan password yang lemah. Serangan Deauther dapat membuat perangkat di jaringan Wi-Fi terputus dari jaringan, sementara serangan beacon dapat membuat perangkat terhubung ke jaringan palsu yang dikendalikan oleh penyerang. Kesimpulan yang didapatkan pada penelitian ini adalah Deauther dan Beacon adalah dua teknik yang digunakan oleh peneliti untuk melakukan serangan peretasan terhadap jaringan Wireless Tenda F3. Deauther merupakan serangan yang memanfaatkan fitur protokol WiFi untuk memaksa perangkat untuk keluar dari jaringan Wireless, sedangkan Beacon adalah teknik membuat jaringan Wireless palsu yang memiliki nama dan konfigurasi yang sama seperti jaringan Wireless asli. Ada beberapa kesimpulan dan saran yang dapat disampaikan penulis sebagai hasil dari evaluasi pengembangan sistem dan laporan akhir ini.

Kata Kunci: Peretasan Jaringan, *Penetration Testing*, *Deauther*, *Beacon*

Abstract− *The internet is very important and has become an important need for people around the world, especially in the current situation. The internet network can be used as a concept where several computers in a university can communicate with each other and can share data and information connected to world connections. Lecturers, employees, and students (users) at one time complained because internet usage was very slow when it was full of users. Due to the excessive use of bandwidth and the lack of proper management of network traffic, it is detrimental to other users. (Prihantoro et al, 2021). YMIK VOCATIONAL SCHOOL had experienced problems with the internet and used the Tenda F3 router and then explained something like the network suddenly dropping and the internet suddenly being slow. According to the statement, the interference was caused by possibly trying to crack the password. From the background description above, the author tries to make a useful research, this hack uses the deauther and beacon methods in hacking wifi*

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

networks. The design of this research is based on a microcontroller, the tool used by the author is NodeMCU ESP8266 for hacking targets using Tenda F3. In research methods to obtain data and information, the methods used in the process of collecting data from various sources are observation, interviews and literature studies with the Deauther and Beacon methods, because the use of these methods is for illegal and unethical purposes. However, researchers can provide information about the results of tests that have been carried out related to this method. Research has been conducted using the Deauther and Beacon methods to test the security of Wi-Fi networks. The results show that this method is very effective in hacking Wi-Fi networks that are not encrypted or protected with weak passwords. Deauther attacks can make devices on a Wi-Fi network disconnect from the network, while beacon attacks can make devices connect to fake networks controlled by attackers. The conclusion obtained in this study is that Deauther and Beacon are two techniques used by researchers to carry out hacking attacks on the Tenda F3 Wireless network. Deauther is an attack that utilizes the WiFi protocol feature to force devices to leave the wireless network, while beacon is a technique for creating fake wireless networks that have the same name and configuration as the original wireless network. There are several conclusions and suggestions that can be conveyed by the author as a result of evaluating the development of the system and this final report.

***Keywords**: Network Hack, Penetration Testing, Deauther, Beacon*

1. PENDAHULUAN

Internet sangat penting dan telah menjadi kebutuhan penting masyarakat di seluruh dunia, terutama dalam situasi saat ini. Jaringan internet bisa dijadikan konsep dimana beberapa komputer dalam suatu Perguruan Tinggi dapat saling berkomunikasi dan dapat berbagi data serta informasi yang terhubung dengan koneksi dunia. Dosen, karyawan, maupun mahasiswa(user) suatu waktu mengeluh karena penggunaan internet sangat lambat jika sedang padat pengguna. Karena adanya penggunaan Bandwidth yang berlebihan dan kurang termanajemennya dengan baik pada traffic jaringan, sehingga merugikan user lain. (Prihantoro dkk, 2021).

Berdasarkan wawancara yang dilakukan di SMK YMIK pada hari senin 03 April 2023, di dapatkan hasil di SMK YMIK, pernah mengalami gangguan pada internet dan menggunakan router Tenda F3 lalu menjelaskan seperti Jaringan tiba tiba putus dan internet lambat tiba tiba. Pihak sekolah tidak mecurigai gangguan tersebut karena adanya peretasan, cuaca atau hal lain karna menurut keterangan karna wireless menggunakan kata sandi yang cukup kuat. Namun akibat dari peretasan jaringan pekerjaan di sekolah mengalami hambatan dan tertunda saat melakukan e learning. Menurut keterangan gangguan tersebut di sebabkan oleh mungkin dengan berusaha membobol kata sandi.

Peneliti bertanya Apakah bapak tau tentang deauther attack dan beacon attack lalu menjawab. Tidak tahu dan tidak penah dengar istilah seperti itu. Tindakan yang dapat dilakukan jika terjadi peretasan jaringan disana adalah cukup dengan mengganti kata sandi secara berkala. Peneliti bertanya bagaimana teknik social engineering dapat digunakan untuk peretasan jaringan, dam menjawab "Saya tau kalo itu mengelabui target nya. Tapi tidak paham dengan hubungannya ke peretasan jaringan". Menanyakan perbedaan antara peretasan jaringan dan penetrasi pengujian dan menjawab Peretasan jaringan menurut nya berusaha masuk ke jaringan kalo penetrasi mereka baru tau juga istilah itu.

Dari uraian latar belakang diatas, maka penulis mencoba untuk membuat suatu penelitian yang bermanfaat, peretasan ini menggunakan metode deauther dan beacon dalam peretasan jaringan wifi. Perancangan penelitian ini berbasis *microcontroller*, alat yang digunakan penulis adalah NodeMCU ESP8266 untuk target peretasannya menggunakan Tenda F3.

2. METODOLOGI PENELITIAN

2.1 Observasi

Observasi adalah metode pengumpulan informasi dengan cara pengamatan atau peninjauan langsung terhadap objek. Dengan Teknik observasi ini dilakukan dengan cara mendatangi tempat

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

studi kasus dan meninjau permasalahan secara langsung yang terjadi di sekolah SMK YMIK. Dengan tujuan observasi ini untuk mendapatkan informasi terkait permasalahan yang ada sehingga dapat mempermudah dalam penyusunan laporan.

2.2 Wawancara

Wawancara ini dilakukan dengan cara melakukan interview dengan staff sekolah menjelaskan tentang permasalahan maupun persoalan yang dirasakan pada SMK YMIK.

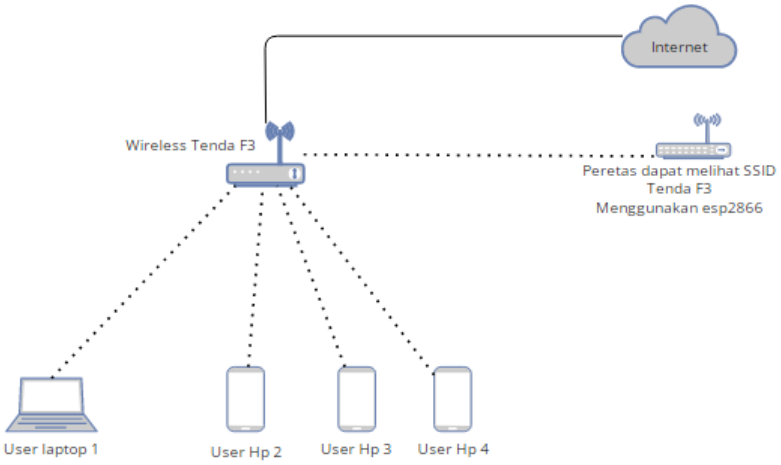
2.3 Studi Pustaka

Pengumpulan data dan informasi tertulis maupun secara teoritis dan empiris yang terkait dengan topik penelitian. Selain itu studi pustaka yang dilakukan peneliti pengumpulan bahan bahan yang terkait dengan judul skripsi melalui buku-buku bacaan dan situs internet, penelitian yang terkait dengan penelitian yang sedang dikembangkan sehingga dapat dimplementasikan dalam penelitian ini.

3. ANALISA DAN PEMBAHASAN

3.1 Skema Jaringan Berjalan

Analisis terhadap jaringan yang berjalan bertujuan untuk mengetahui lebih jelas bagaimana cara kerja dari jaringan tersebut dan masalah apa saja yang sedang dihadapi jaringan tersebut untuk dapat dijadikan usulan perancangan jaringan.



Gambar 1. Skema Jaringan Berjalan

3.2 Topologi Jaringan Berjalan

Topologi jaringan yang berjalan ialah menggunakan topologi *Basic Service Set* (BSS), di karnakan tujuannya adalah Koneksi antar *wireless client* pada topologi ini diperantarai oleh sebuah perangkat *access point*. Setiap *wireless client* yang ingin terhubung dengan *client* lainnya harus terhubung terlebih dahulu dengan *access point* yang digunakan.

3.3 Arsitektur Jaringan Berjalan

Arsitektur jaringan yang ada pada wireless Tenda F3 membuka SSID nya ke area publik dan dapat di akses oleh siapapun yang belum terhubung pada jaringan tersebut, dan frekuensi nya masih menggunakan 2.4Ghz yang berdampak akan terlihat oleh alat esp 2886 milik peretas, efek dari terbukanya SSID dan frekuensi 2.4Ghz maka bisa terserang dengan metode *deauther* dan *beacon* menjadikan semua yang terhubung pada *wireless* tersebut akan lumpuh atau putus koneksi, dan peretas membuat *wireless* tiruan untuk mengelabui para *user* agar membingungkan dan susah membedakan *wireless* yang asli atau bukan. Dan bahayanya peretas jika mendapat akses ke *wireless* Tenda F3 bisa mengatur konfigurasi di dalam *access point* tersebut.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

3.4 Analisa Jaringan Usulan

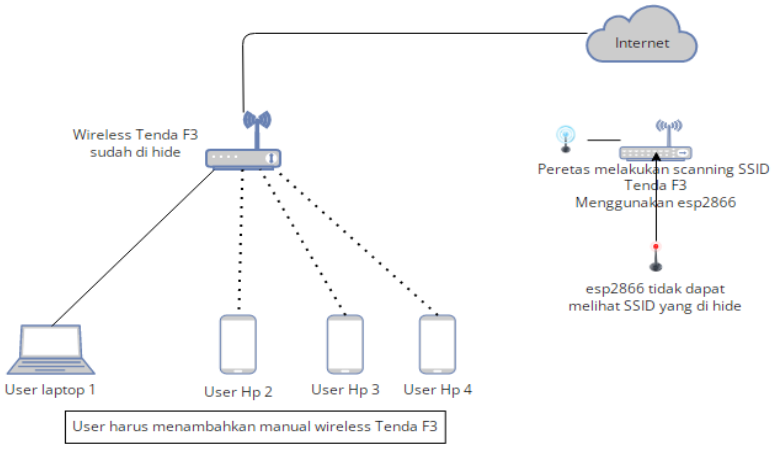
Setelah penulis menganalisa jaringan berjalan ini, maka penulis mengajukan penelitian implementasi peretasan jaringan menggunakan alat esp 8266 dengan teknik *penetration testing* metode *deauther* dan *beacon* pada *wireless* Tenda F3. dikarenakan jaringan pada *wireless* tersebut masih kurang aman jika SSID di tampilkan ke area publik.

3.5 Topologi Jaringan Usulan

Untuk topologi jaringan penulis mengubah menggunakan topologi *Extended Service Set* (ESS), di karnakan tujuannya adalah untuk menjangkau area yang lebih jauh lagi. Jadi, bisa dikatakan topologi ESS ini merupakan gabungan atau kumpulan dari topologi BSS. Pada topologi BSS atau ESS, kita bisa memadukannya dengan jaringan kabel. Koneksi ini biasa disebut infrastruktur, dimana *wireless client* dapat terhubung dan berkomunikasi dengan *client* lain pada jaringan kabel.

3.6 Skema Jaringan Usulan

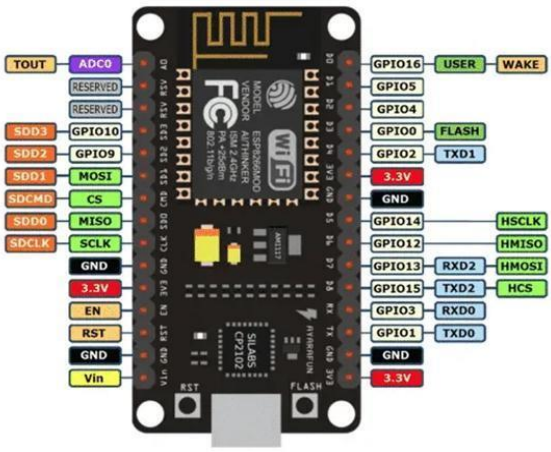
Dengan permasalahan yang ada maka penulis memberikan usulan konfigurasi *access point* pada *wireless* Tenda F3. Berikut ini skema jaringan usulan.



Gambar 2. Skema Jaringan Usulan

4. IMPLEMENTASI

4.1 Implementasi NodeMCU (board v.3 Lolin) ESP8266



Gambar 3. NodeMCU (board v.3 Lolin) ESP8266

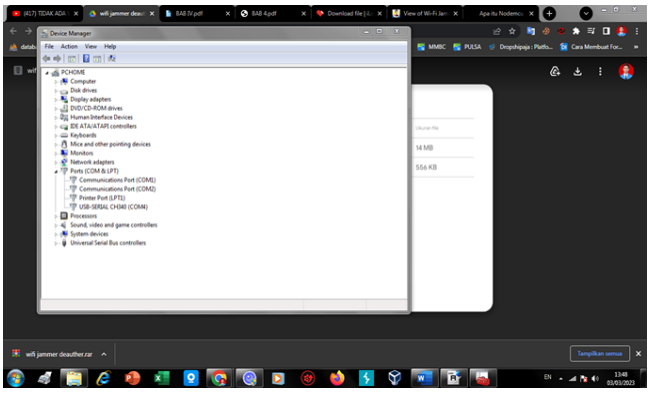
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

Gambar 4. NodeMCU

4.2 Implementasi Konfigurasi

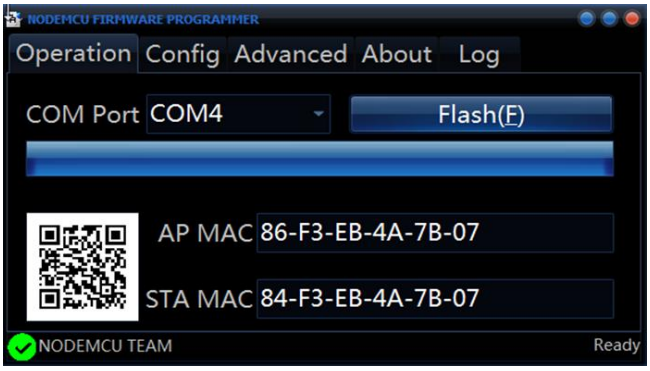
4.2.1 Implementasi ESP 8266

a. *Install* CH240G driver



Gambar 5. Install CH240G driver

b. *Flash* ESP 8266



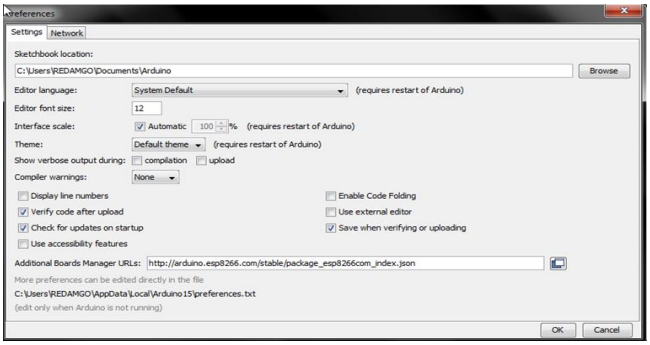
Gambar 6. Flash ESP 8266

c. Program Ardiuno

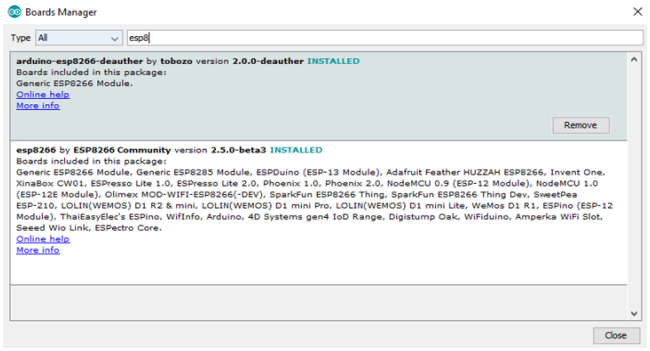
Gambar 7. Program Arduino

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

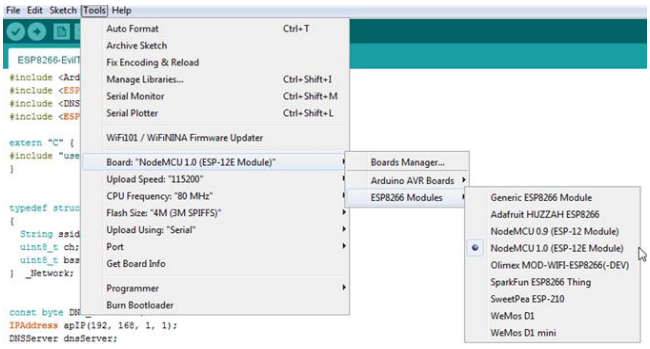
d. *Setting* program Arduino



Gambar 8. *Setting* program Arduino

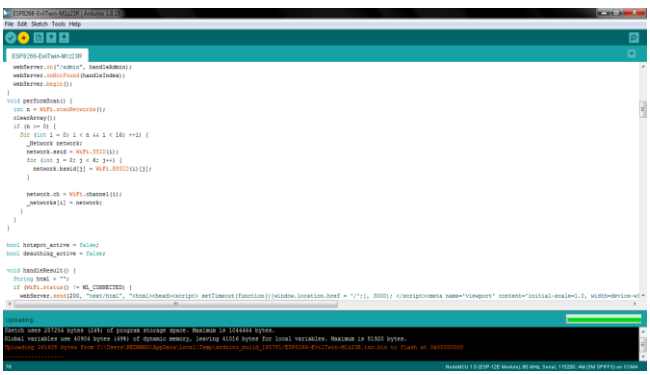


Gambar 9. Arduino Module Install



Gambar 10. *Setting Board* NodeMCU

e. Proses *Upload Script*

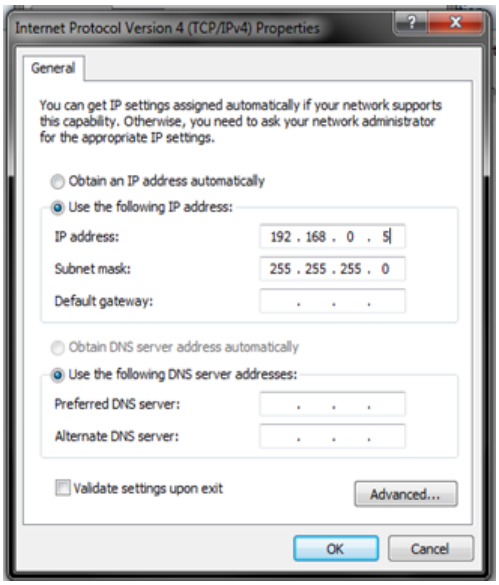


Gambar 11. Proses Upload Script

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

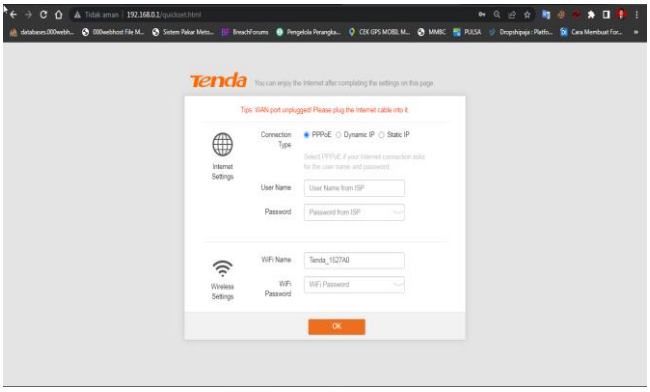
4.2.2 Konfigurasi TP-LINK WR840N

a. ***Setting ip address computer***



Gambar 12. Setting ip address computer

b. Buka browser konfigurasi



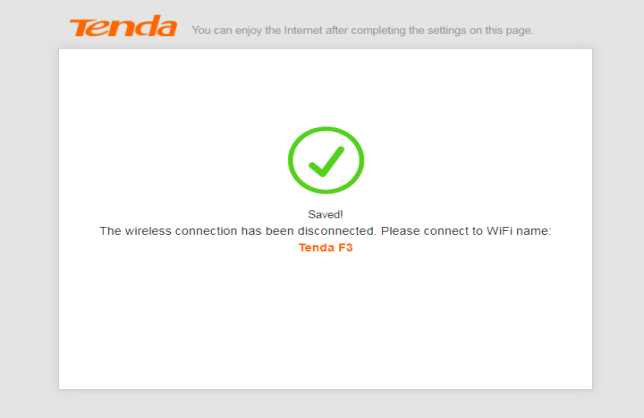
Gambar 13. Browser Konfigurasi

c. Pilih Menu *Connection Type*

Gambar 14. Menu Connection Type

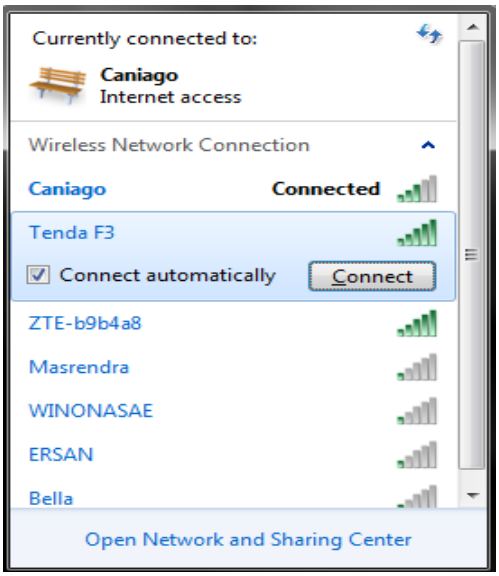
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

d. Menu *Save*



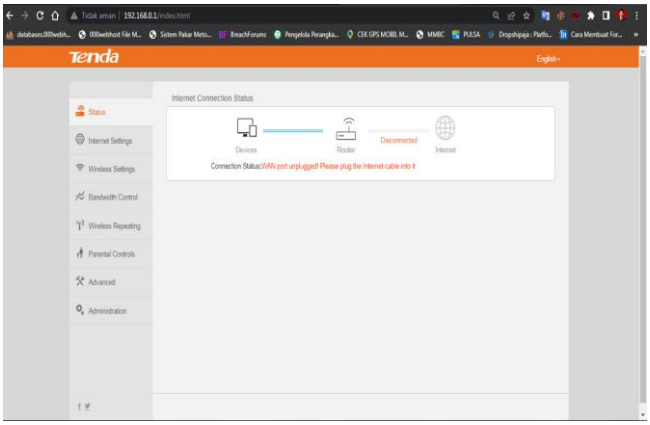
Gambar 15. Menu *Save*

e. Pilih *Wireless* Tenda F3



Gambar 16. Pilih *Wireless* Tenda F3

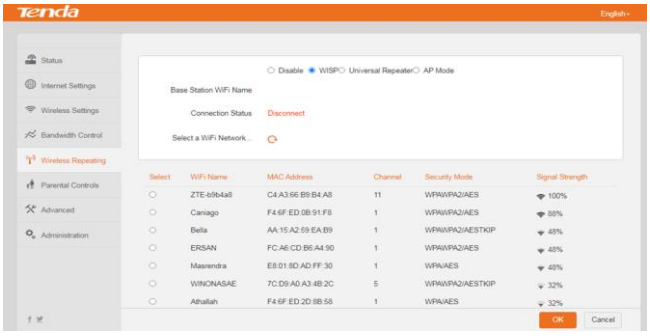
f. Menu Halaman Fitur Utama Tenda F3



Gambar 17. Menu Halaman Fitur Utama Tenda F3

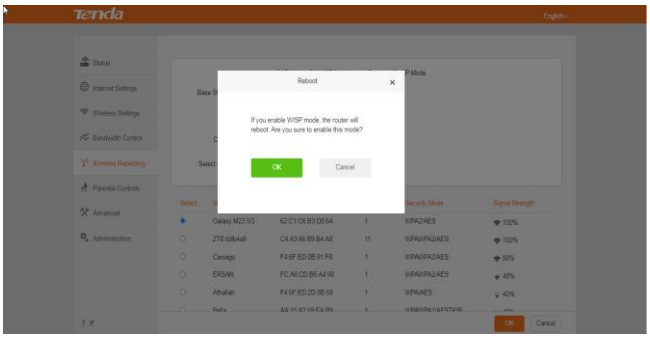
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

g. *Setting Menu* WISP



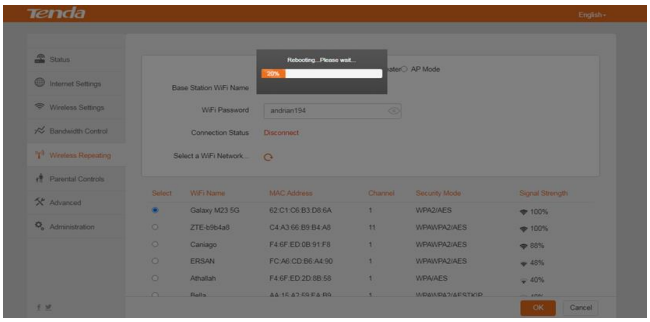
Gambar 18. Setting Menun WISP

h. *Save Setting* WISP



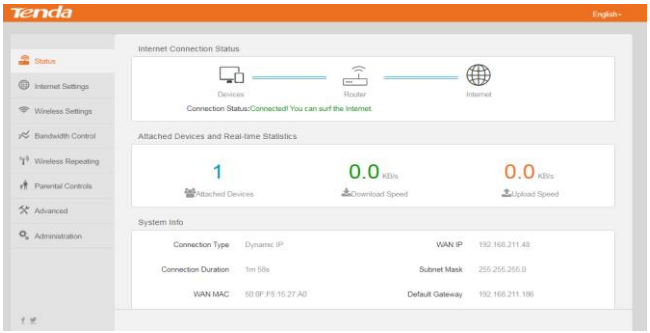
Gambar 19. Save Setting WISP

i. *Rebooting*



Gambar 20. *Rebooting*

j. Tenda F3 Berhasil Mendapat Akses Internet



Gambar 21. Tenda F3 Berhasil Mendapat Akses Internet

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

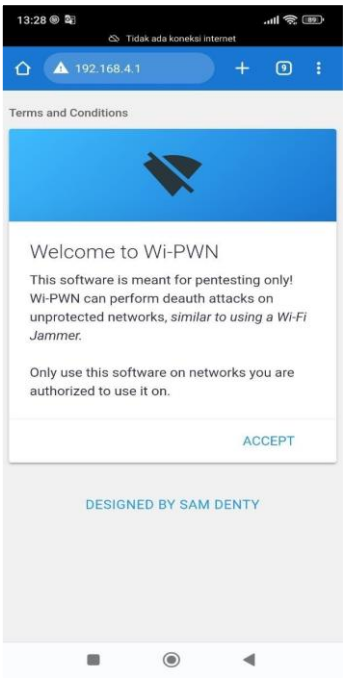
4.3 Implementasi Pengujian

4.3.1 Implementasi Pengujian Metode *Deauther*

a. Masuk Wifi Wi-PWN

Gambar 22. Masuk Wifi Wi-PWN

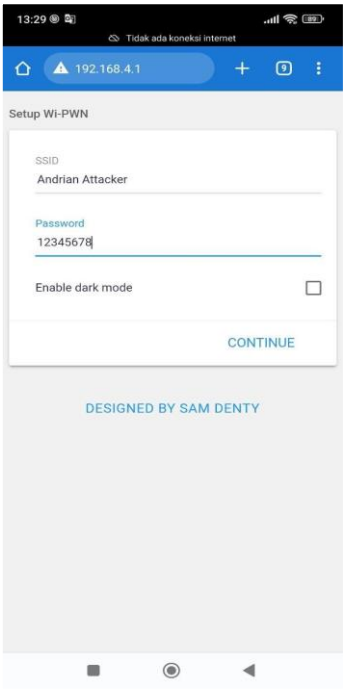
b. Halaman Utama Software Wi-PWN



Gambar 23. Halaman Utama Software Wi-PWN

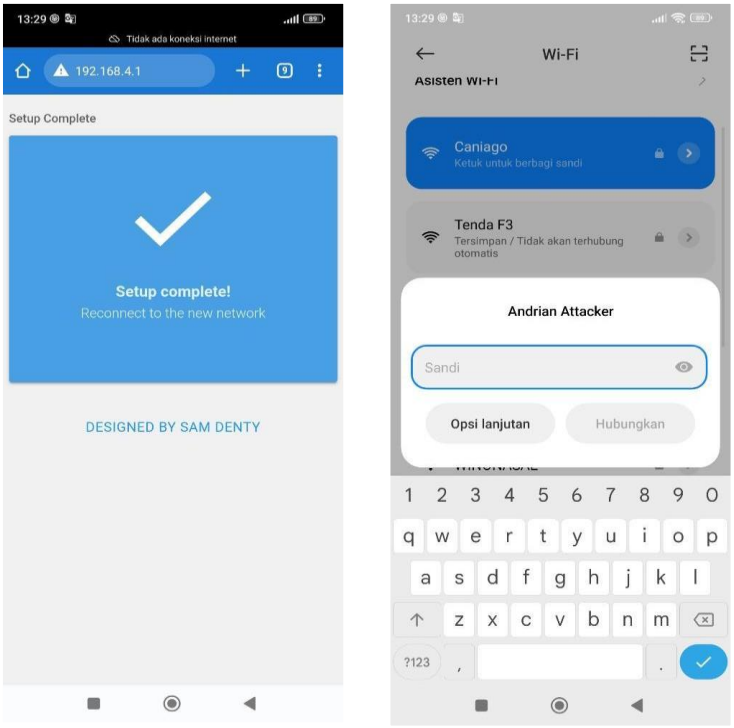
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

c. *Setting* SSID Pada Alat ESP 2866



Gambar 24. *Setting* SSID Pada Alat ESP 2866

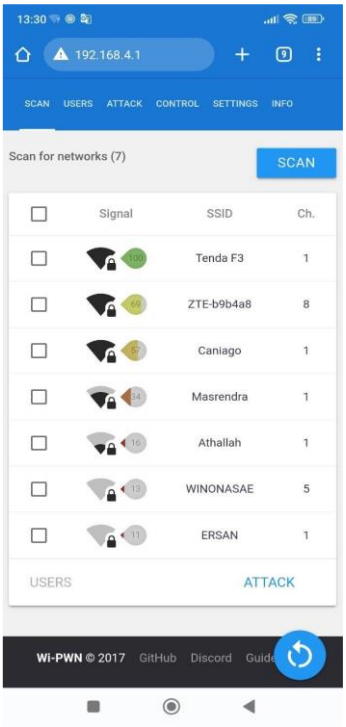
d. SSID Berubah Menjadi Andrian Attacker



Gambar 25. SSID Berubah Menjadi Andrian Attacker

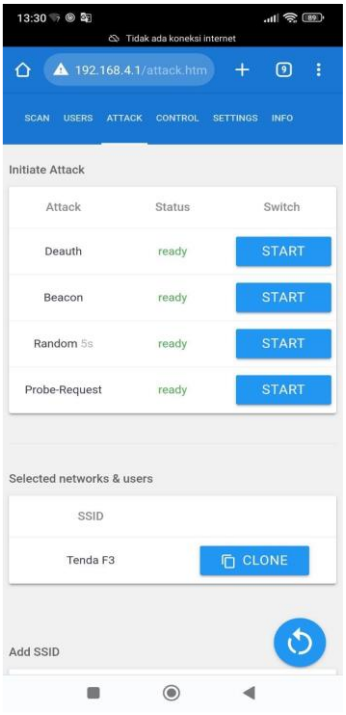
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

e. Tampilan Menu Scan



Gambar 26. Tampilan Menu Scan

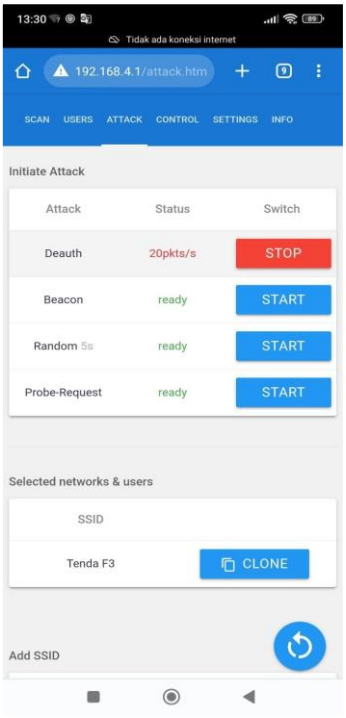
f. Tampilan Menu *Attack*



Gambar 27. Tampilan Menu *Attack*

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

g. Tampilan *Deauther Attack*



Gambar 28. Tampilan *Deauther Attack*

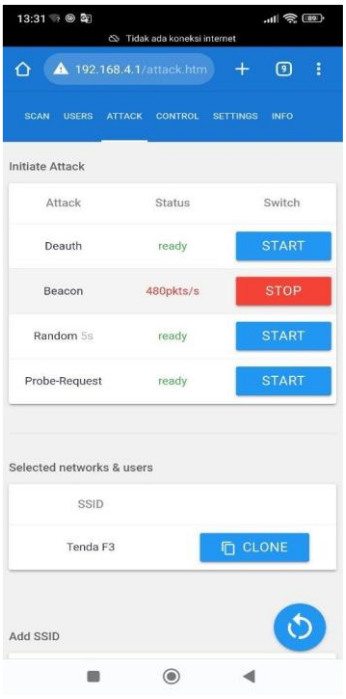
h. Tampilan Hasil *Deauther Attack*

Gambar 29. Tampilan Hasil *Deauther Attack*

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

4.3.2 Implementasi Pengujian Metode *Beacon*

a. Tampilan *Beacon Attack*



Gambar 30. Tampilan *Beacon Attack*

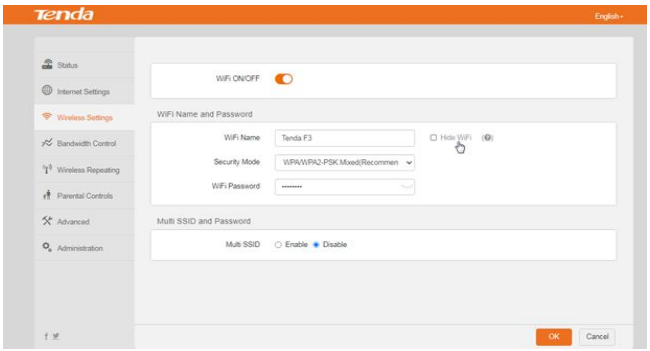
b. Tampilan Hasil *Beacon Attack*

Gambar 31. Tampilan Hasil *Beacon Attack*

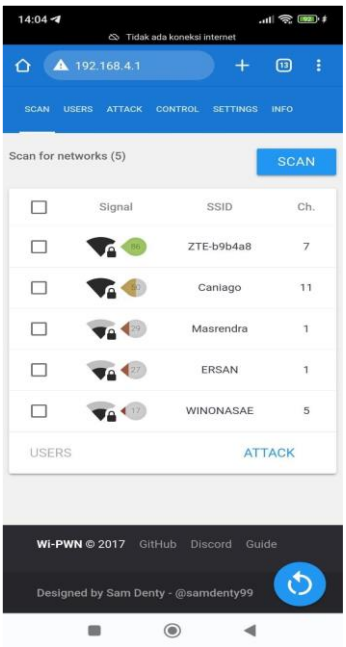
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

4.3.3 Implementasi Pengamanan

a. Implementasi pengamanan Tenda F3



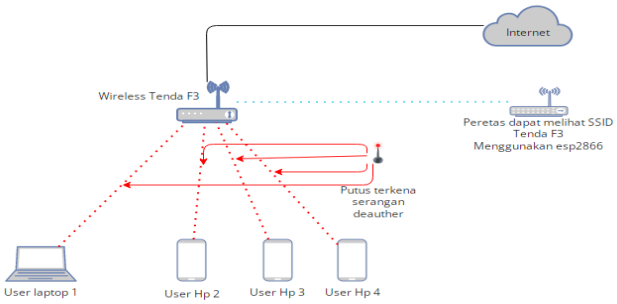
Gambar 32. *Implementasi pengamanan Tenda F3*



Gambar 33. *ESP 2866 Tidak Dapat Scanning Wireless Yang di Hide*

4.4 Kasus dan Hasil pengujian

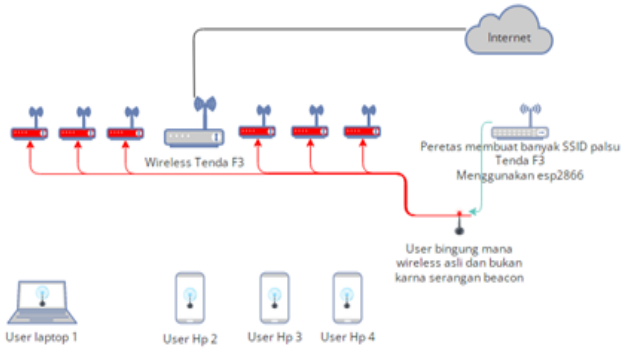
4.4.1 Kasus Pengujian *Deauther*



Gambar 34. Kasus Pengujian Metode *Deauther*

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

4.4.2 Kasus Pengujian *Beacon*



Gambar 35. Kasus Pengujian Metode *Beacon*

4.4.3 Hasil Pengujian Dengan Metode *Deauther* Dan *Beacon*

Penelitian telah dilakukan dengan menggunakan metode *Deauther* dan *Beacon* untuk menguji keamanan jaringan Wi-Fi. Hasilnya menunjukkan bahwa metode ini sangat efektif dalam meretas jaringan Wi-Fi yang tidak dienkripsi atau dilindungi dengan password yang lemah. Serangan *Deauther* dapat membuat perangkat di jaringan Wi-Fi terputus dari jaringan, sementara serangan *Beacon* dapat membuat perangkat terhubung ke jaringan palsu yang dikendalikan oleh penyerang.

5. KESIMPULAN

Kesimpulan yang didapatkan pada penelitian ini adalah *Deauther* dan *Beacon* adalah dua teknik yang digunakan oleh peneliti untuk melakukan serangan peretasan terhadap jaringan *Wireless* Tenda F3. *Deauther* merupakan serangan yang memanfaatkan fitur protokol WiFi untuk memaksa perangkat untuk keluar dari jaringan *Wireless*, sedangkan *Beacon* adalah teknik membuat jaringan *Wireless* palsu yang memiliki nama dan konfigurasi yang sama seperti jaringan *Wireless* asli. Ada beberapa kesimpulan dan saran yang dapat disampaikan penulis sebagai hasil dari evaluasi pengembangan sistem dan laporan akhir ini.

REFERENCES

Vinka, Maria, Angela, Nicoline, Michele. (2021). Pengaruh Teknologi Internet Terhadap Pengetahuan Masyarakat Jakarta Seputar Informasi Vaksinasi Covid-19. TEMATIK (*Jurnal Teknologi Informasi dan Komunikasi*), Vol. 8, No. 1, Juni 2021, E-ISSN : 2443-3640.

Prihantoro, Cahyo, Hidayah, Kharisma, Agung, Fernandez, Sandhy.(2021). Analisis Manajemen Bandwidth Menggunakan Metode Queue Tree pada Jaringan Internet Universitas Muhammadiyah Bengkulu. JUST TI (*Jurnal Sains Terapan Teknologi Informasi*), Vol. 13, No. 2, Juli 2021, 2021): 81-86 E-ISSN: 2579-4510 ISSN: 2085-6458.

Rachmie, Synthiana. (2020). Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website. *Jurnal Litigasi*, Vol. 21 April 2020, e-ISSN: 2442-2274.

Zulfitria, Ansharullah , Fadhillah, Rastia. Penggunaan Teknologi Dan Internet Sebagai Media Pembelajaran Di Masa Pandemi Covid-19. *Prosiding Seminar Nasional Penelitian LPPM UMJ*, 7 Oktober 2020, E-ISSN: 2745-6080.

Wicaksana, Hasan, Sahrial, Saedudin, Rohmat, Fathinuddin, Muhammad. (2022). Perancangan Infrastruktur Teknologi Informasi Adaptif Dengan Metode Ppdioo Untuk Mendukung Implementasi Sistem Informasi Manajemen Puskesmas. *e-Proceeding of Engineering*, Vol.9, No.2 April 2022, ISSN : 2355-9365.

Hidayat, Nur, Muhammad, Andi. (2021). Sistem Deteksi Intrusi Dan Prevensi Berbasis Open Source. Jurnal INSTEK (*Informatika Sains dan Teknologi*), Volume 6 Nomor. 1, April 2021, E-ISSN : 2581-1711.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 5, Mei 2024
ISSN 2828-2442 (media online)
Hal 1276-1292

Dasanty, Vriella, Laras, Dermawan, Arwin, Dodik. (2020). Studi Literatur Monitoring Manajemen Jaringan Internet Dengan Konsep Snmp Terhadap Akses Siswa. *Jurnal IT-EDU*. Volume 5 Nomor 1 Tahun 2020, 38-48, E-ISSN : 2540-9263.

Najib, Warsun, Sulistyo, Selo, Widyawan. (2020). Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, Vol. 9, No. 4, November 2020, ISSN 2301 – 4156.

Manuaba, Hendrawan, Verry, Bagus, Ida, Hidayat, Risanuri, Kusumawardani, Suning, Sri. (2012). Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus : Kantor Pusat Fakultas Teknik Universitas Gadjah Mada). *JNTETI*, Vol. 1, No. 1, Mei 2012, ISSN 2301 – 415613.

Saputro, Ardiyansyah, Vian, Raharjo, Suwanto. (2022). Pengaruh Penggunaan Beacon Interval Dalam Meningkatkan Throughput Jaringan Wireless IEEE 802.11ax. *Jurnal Sistem Komputer dan Kecerdasan Buatan*, Vol.VI No.1 September Tahun 2022, ISSN: 2621 – 2927.