OKTAL : OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 4, April 2024
ISSN 2828-2442 (media online
Hal 885-899

Implementasi Pengamanan Jaringan Dengan Teknik *Penetration Testing* Menggunakan Metode *Deauther* Dan *Evil Twin Pada Wireless* Tl-WR840N

Eka Rahmat Mauluddin[1*], Teti Desyani[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*]ekarahmamauluddin522@email.com, [2]dosen00839@unpam.ac.id
(* : coressponding author)

Abstrak−Jaringan komputer berkembang dengan sangat pesat, baik di instansi-instansi komersil, dunia akademik,bahkan rumah-rumah penduduk yang membutuhkan akses internet. Internet diakses oleh banyak orang tanpa terkecuali hacker dan cracker. Berbagai Issu keamanan jaringan saat ini menjadi sangat penting dan patut untuk diperhatikan. Sebuah jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para hacker, baik jaringan wired LAN maupun wireless LAN. Pada saat proses pengiriman data akan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menyadap atau mengubah data tersebut. Dalam hal ini, perlu dilakukan implementasi pengamanan jaringan dengan teknik penetration testing menggunakan metode Deauther dan evil twin pada wireless Tl-WR840N. Hasil analisis yang didapatkan setelah melakukan pengujian dengan metode Deauther dan Evil twin adalah metode ini sangat efektif dalam meretas jaringan Wi-Fi yang tidak dienkripsi atau dilindungi dengan password yang lemah. Dalam pengujian metode Deauther dan Evil Twin berhasil meretas jaringan Wi-Fi dengan tingkat keberhasilan yang cukup tinggi. Oleh karena itu, sangat penting bagi pengguna jaringan WiFi untuk menjaga keamanannya dengan menggunakan teknologi keamanan yang tepat, seperti penggunaan kata sandi yang kuat dan enkripsi data.

Kata Kunci: Pengamanan Jaringan, *Penetration Testing*, *Deauther*, *Evil Twin*

Abstract− *Computer networks are growing very rapidly, both in commercial institutions, in the academic world, and even in people's homes that need internet access. The internet is accessed by many people without exception to hackers and crackers. Various network security issues are currently very important and deserve attention. A network connected to the internet is basically insecure and can always be exploited by hackers, both wired LAN and wireless LAN networks. During the process of sending data, it will pass through several terminals to arrive at the destination, which means it will provide an opportunity for other users who are not responsible to intercept or change the data. In this case, it is necessary to implement network security with penetration testing techniques using the Deauther and evil twin methods on the Tl-WR840N wireless. The results of the analysis obtained after testing with the Deauther and Evil twin methods are that this method is very effective in hacking Wi-Fi networks that are not encrypted or protected with weak passwords. In testing the Deauther and Evil Twin methods managed to hack the Wi-Fi network with a fairly high success rate. Therefore, it is very important for WiFi network users to maintain their security by using the right security technologies, such as using strong passwords and data encryption.*

Keywords*: Network Security, Penetration Testing, Deauther, Evil Twin*

1. PENDAHULUAN

Jaringan komputer berkembang dengan sangat pesat, baik di instansi-instansi komersil, dunia akademik, bahkan rumah-rumah penduduk yang membutuhkan akses internet. Internet diakses oleh banyak orang tanpa terkecuali hacker dan cracker. Dengan alasan tertentu mereka melakukan penyusupan yang dapat merugikan para pemilik server dan jaringan komputer. Mereka menggunakan berbagai macam serangan jaringan komputer dengan tools yang dibuat secara mandiri ataupun yang telah ada di pasar. Efek utama dari serangan jaringan komputer berupa lambatnya akses internet. Selain itu untuk jenis serangan jaringan yang sangat berbahaya dapat mengakibatkan rusaknya data pada server, sehingga hal ini sangat merugikan pengguna ataupun *end user* yang sedang mengakses. Umumnya kejahatan internet dimulai dengan mengeksploitasi host-host dan jaringan komputer sehingga para penyusup datangmelintasi jaringan, terutama jaringan yang berbasis TCP/IP. (Setyawan, Okki, dkk, 2021).

OKTAL : OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 4, April 2024
ISSN 2828-2442 (media online
Hal 885-899

Berbagai Issu keamanan jaringan saat ini menjadi sangat penting dan patut untuk diperhatikan. Sebuah jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para hacker, baik jaringan wired LAN maupun wireless LAN. Dalam perancangan sebuah system keamanan jaringan yang handal maka perlu dipahami dengan baik melalui prosess analisa yang tepat sehingga system keamanan jaringan yang terhubung ke internet nantinya dapat berjalan efektif dan meminimalisir terjadinya serangan-serangan oleh para *hacker*. *Ettercap* adalah *tools packet sniffer* yang dipergunakan untuk menganalisa protokol jaringan dan mengaudit keamanan jaringan.

Dilansir dari website cnbcindonesia Dalam konteks keamanan informasi, khususnya keamanan jaringan, hal ini bisa disebut dengan serangan *spoofing*, yaitu situasi dimana seseorang atau program berhasil menyamar sebagai orang lain dengan memalsukan data, untuk mendapatkan keuntungan yang tidak sah. Biasanya hacker yang meniru hal ini menggunakan USB ukuran kecil untuk memancarkan WiFi tiruan. Walaupun jaringan WiFi tiruan, orang bisa dengan mudah langsung terkoneksi.

Pada website Mentari Isp Indramayu, Pengetahuan netizen Indonesia tentang *cyber security* masih kurang Dari enam negara yang disurvei Mentari Isp Indramayu - Peringkat *Cyber Security* Indonesia, Indonesia menempati posisi kedua terbawah dalam hal pengetahuan terkait *cyber security*. Salah satu faktor penyebabnya adalah karena kurangnya edukasi terkait isu tersebut, khususnya di ranah ranah edukasi formal.

Dari uraian latar belakang diatas, maka penulis mencoba untuk membuat suatu penelitian yang bermanfaat, pengetesan ini menggunakan metode *Deauther* dan *Evil Twin* dalam pengetesan pada jaringan wifi TL-WR840N. Perancangan penelitian ini berbasis alat, adapun alat yang digunakan penulis adalah NodeMCU esp 8266 untuk bahan test nya menggunakan TPLINK TL-WR840N.

2. METODOLOGI PENELITIAN

2.1 Metode Perancangan Jaringan

Metode yang digunakan pada penelitian ini berdasar pada metode PPDIOO (*Prepare, Plan, Design, Implement, Operate dan Optimize*) dari CCNA. Berikut adalah penjelasan dari langkah-langkah metode PPDIOO yang disesuaikan dengan prosedur kerja penelitian :

1. Persiapan (Prepare) Pada tahap ini, dilakukan pengumpulan data yang dibutuhkan untuk keperluan penelitian di RSU. Sari Mutiara Lubuk Pakam.
2. Perencanaan (Plan) Melakukan identifikasi terhadap apa yang diperlukan oleh RSU. Sari Mutiara Lubuk Pakam (Gap Analysis). Pada tahap ini juga sudah dilakukan perancangan sederhana topologi jaringan.
3. Desain (Design) Pada tahap ini, rancangan sederhana yang telah dibuat akan didesain ulang dengan menggunakan sebuah aplikasi desain topologi, sehingga gambaran topologi sudah bisa dijelaskan secara rinci kepada pihak manajemen. Desain jaringan yang telah dibuat haruslah memiliki kehandalan, keamanan dan kinerja yang baik.
4. Implementasi (Implement) Pada tahap ini, desain yang telah dibuat akan diajukan ke pihak manajemen untuk disetujui dan dilaksanakannya instalasi. Simulasi jaringan juga sudah dilakukan disini sebelum dismantle (pembongkaran) kabel dilakukan.
5. Pelaksanaan (Operate) Melakukan testterhadap arsitektur jaringan yang telah dipasang. Pada tahap ini, akan diadakan penilaian apakah desain yang ditetapkan sudah sesuai kebutuhan pihak Rumah Sakit.
6. Optimisasi (Optimize) Pada tahap ini, akan dilakukan manajemen jaringan guna mempertahankan kualitas. Manajemen bandwidth berada pada tahap ini.

2.2 Metode Pengumpulan Data

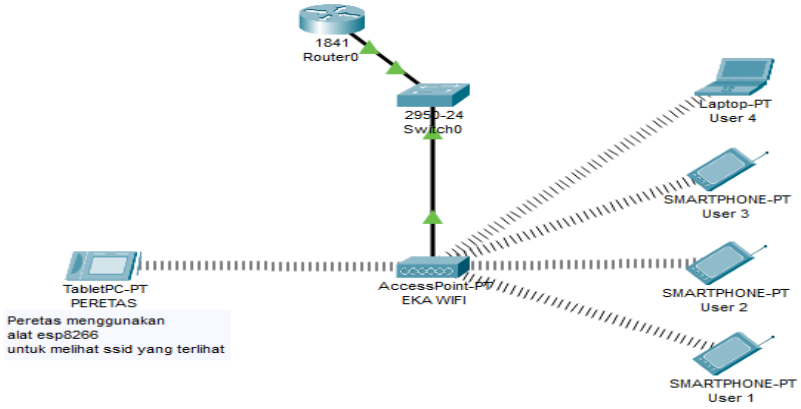
Metode pengumpulan data dengan cara study literature, yaitu dengan memahami masalah dan melakukan pengumpulan data dari artikel-artikel, karya ilmiah, buku-buku, dokumen, serta cetakan yang bersumber dari internet.

OKTAL : OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 4, April 2024
ISSN 2828-2442 (media online
Hal 885-899

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

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 alat TP-LINK WR840N membuka SSID nya ke public 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 *Evil Twin* menjadikan semua yang terhubung pada *wireless* tersebut akan lumpuh atau putus koneksi, dan peretas membuat *wireless* tiruan untuk mengelabui para *user* agar memasukan kata sandi *wireless* tersebut. Peretas jika dapat akses ke TP-LINK WR840N bisa mengatur konfigurasi di dalam *access point* tersebut.

3.4 Analisa Jaringan Usulan

Setelah penulis menganalisa jaringan berjalan ini , maka penulis mengajukan penelitian Implementasi Pengamanan Jaringan Dengan Teknik *Penetration Testing* Menggunakan Metode *Deauther* Dan *Evil Twin* Pada *Wireless* TL-WR840N. Dikarnakan Jaringan pada *Wireless* tersebut masih kurang aman jika SSID di tampilkan ke *public*.

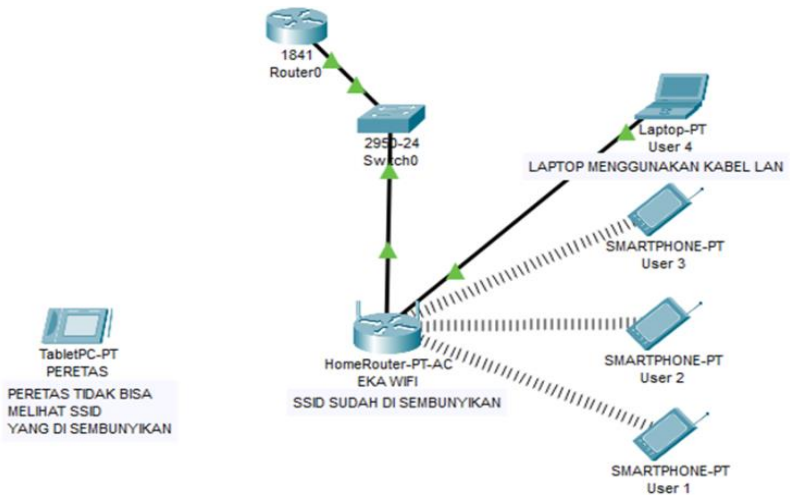
3.5 Topologi Jaringan Usulan

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 wireless pada TP-LINK TL-WR840N. Berikut ini skema jaringan usulan.

OKTAL : OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 4, April 2024
ISSN 2828-2442 (media online
Hal 885-899



Gambar 2. Skema Jaringan Usulan

3.7 Spesifikasi *Hardware*

Dari hasil analisa yang di lakukan penulis terhadap jaringan. Penulis menjelaskan tentang spesifikasi perangkat jaringan yang di gunakan sebagai berikut

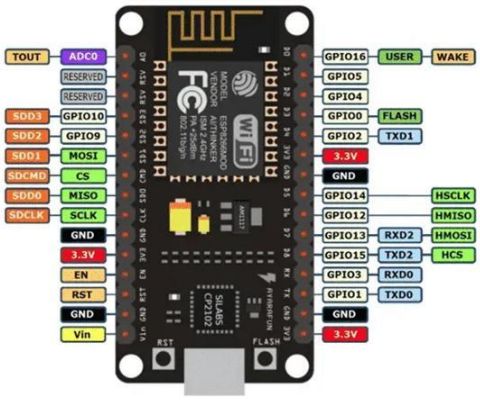
Tabel 1. Spesifikasi *Hardware*

No.	Hardware	Model	Gambar
1	tp-link	TL-WR840N	
2	Wemos lolin NodeMcu V3	ESP2866	
3	LAN	STRAIGHT	
4	Laptop		
5	Smartphone		

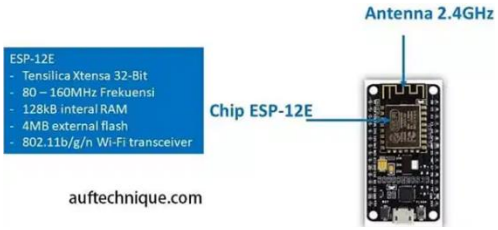
OKTAL : OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 4, April 2024
ISSN 2828-2442 (media online
Hal 885-899

4. IMPLEMENTASI

4.1 Implementasi NodeMCU (board v.3 Lolin) ESP8266



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

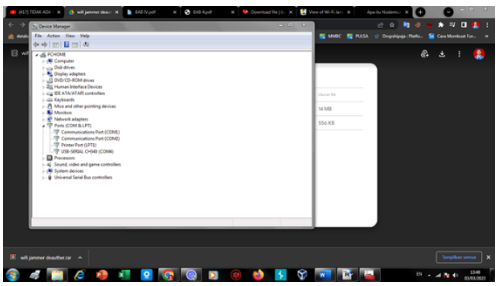


Gambar 4. *ESP-12E*

4.2 Implementasi Konfigurasi

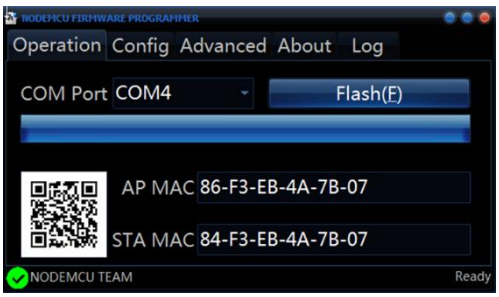
4.2.1 Konfigurasi ESP 8266

a. *Install* CH240G Driver



Gambar 5. *Install CH240G driver*

b. *Flash* ESP 8266



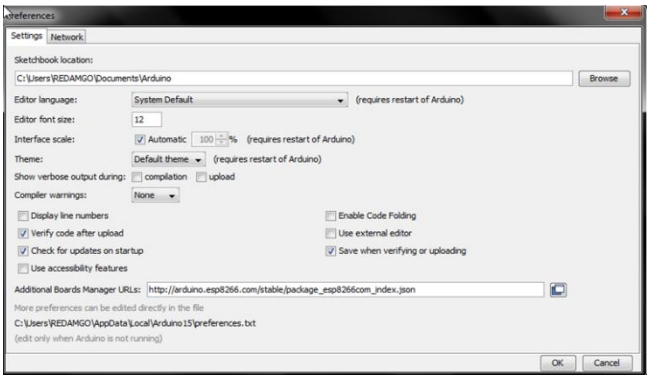
Gambar 6. Flash ESP 8266

OKTAL : OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 4, April 2024
ISSN 2828-2442 (media online
Hal 885-899

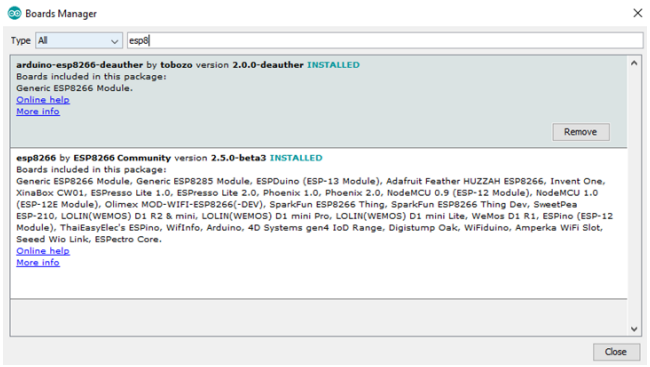
c. Program Ardiuno

Gambar 7. Program Ardiuno

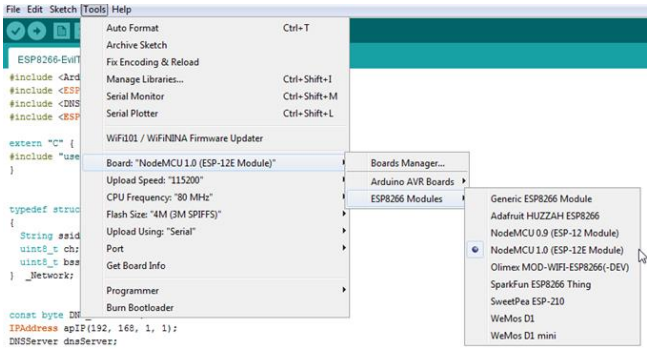
d. *Setting* Program Arduino



Gambar 8. Setting Program Arduino



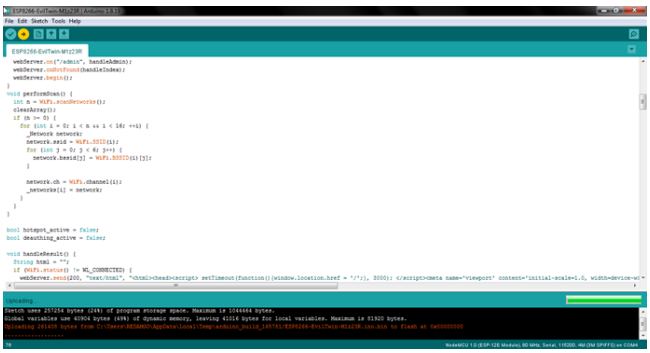
Gambar 9. *Boards Manager*



Gambar 10. *Setting Board* NodeMCU

OKTAL : OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 4, April 2024
ISSN 2828-2442 (media online
Hal 885-899

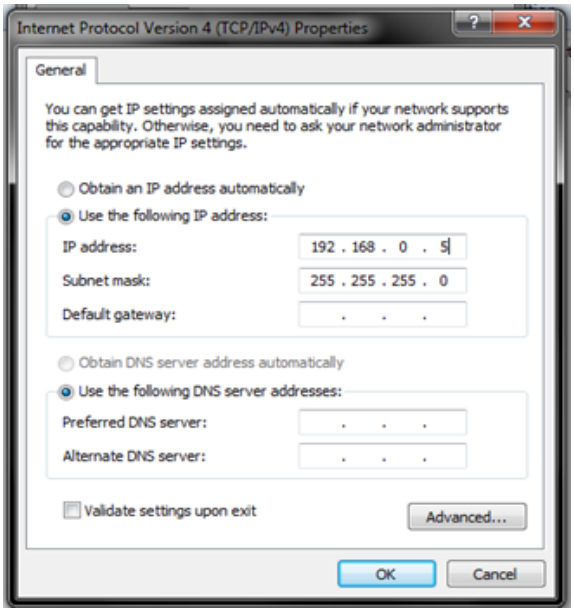
e. Proses *Upload Script*



Gambar 11. Proses *Upload Script*

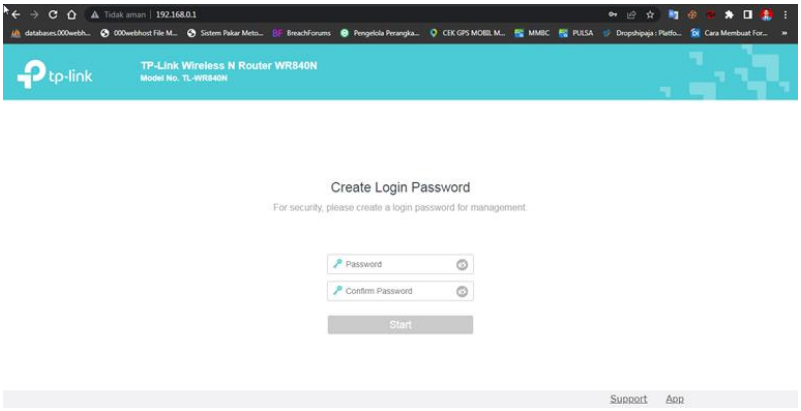
4.2.2 Konfigurasi TP-LINK WR840N

a. *Setting ip address computer*



Gambar 12. Setting ip address computer

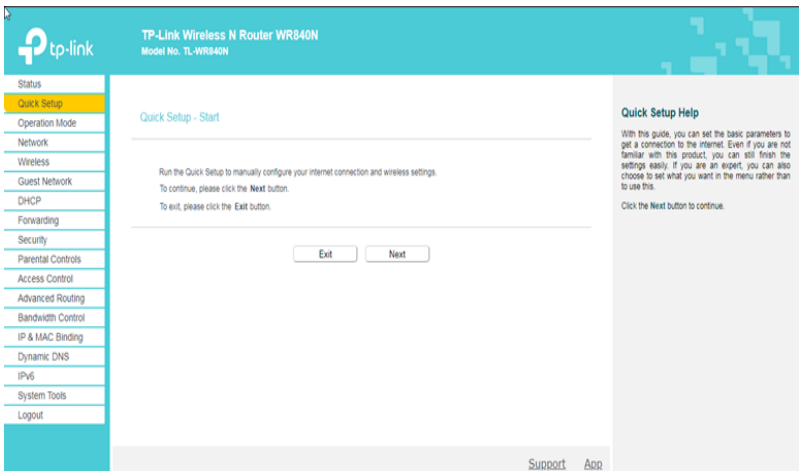
b. Buka browser konfigurasi



Gambar 13. Buka *Browser* Konfigurasi

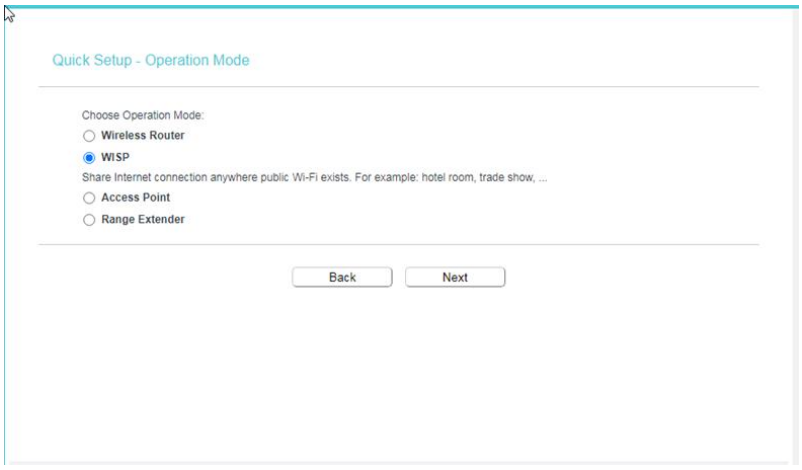
OKTAL : OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 4, April 2024
ISSN 2828-2442 (media online
Hal 885-899

c. ***Quick Setup***



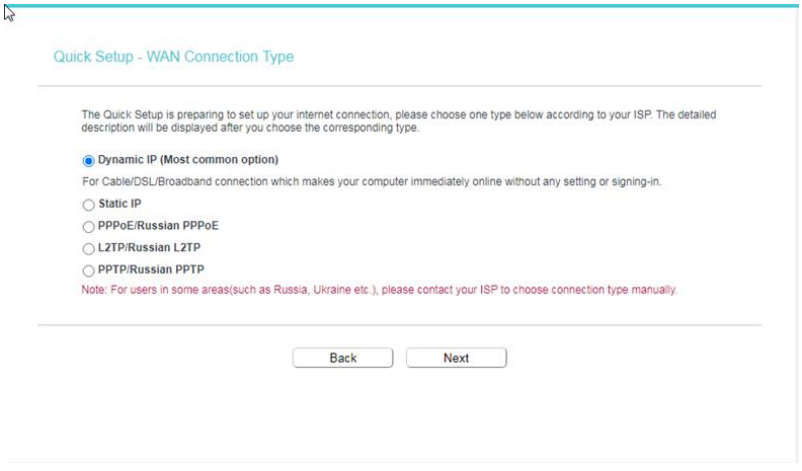
Gambar 14. *Quick Setup*

d. ***Operating Mode***



Gambar 15. *Operating Mode*

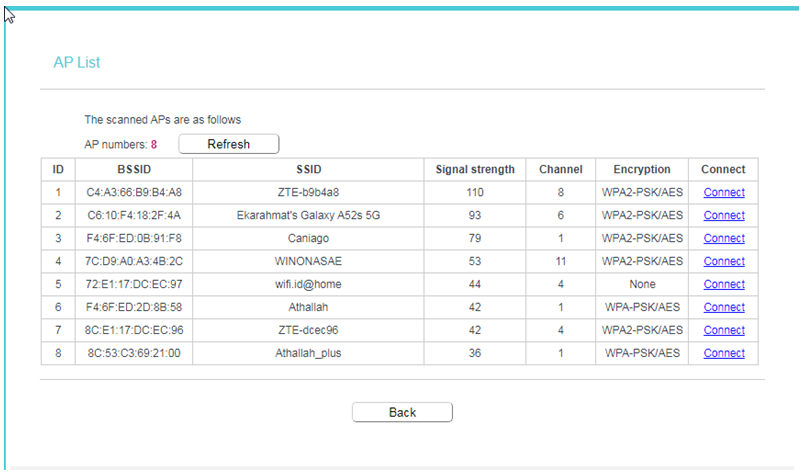
e. **WAN *Connection Type***



Gambar 16. *WAN Connection Type*

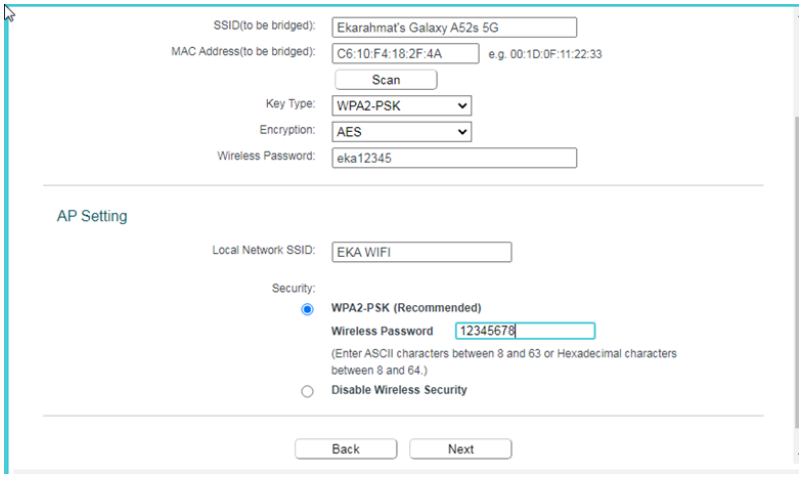
OKTAL : OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 4, April 2024
ISSN 2828-2442 (media online
Hal 885-899

f. Pilih *Access Point*



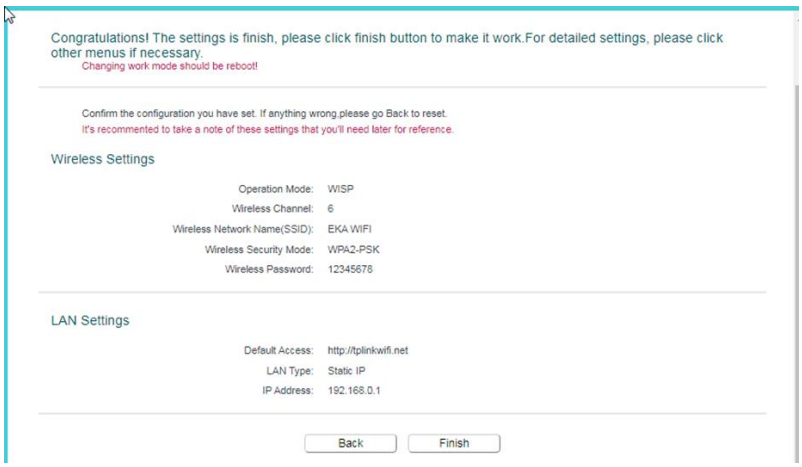
Gambar 17. Pilih *Access Point*

g. *Setting* WISP



Gambar 18. *Setting* WISP

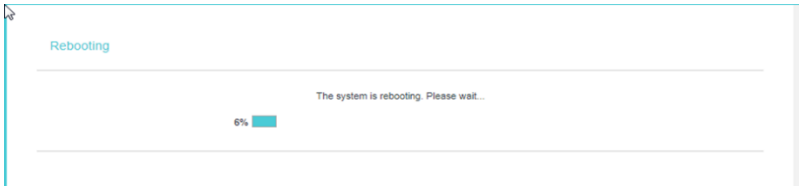
h. *Save Setting* WISP



Gambar 19. *Save Setting* WISP

OKTAL : OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 4, April 2024
ISSN 2828-2442 (media online
Hal 885-899

i. *Rebooting*



Gambar 20. *Rebooting*

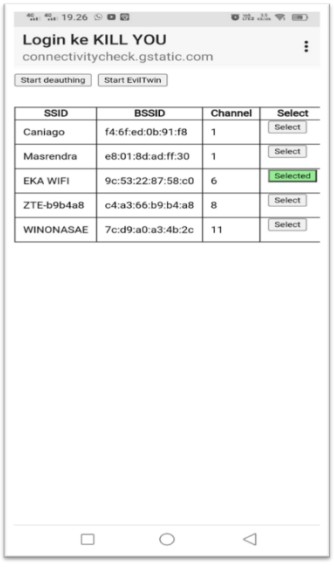
4.3 Implementasi Pengujian

4.3.1 Implementasi Pengujian Metode Deauther

a. Halaman *Dasboard*

Gambar 21. Halaman *Dasboard*

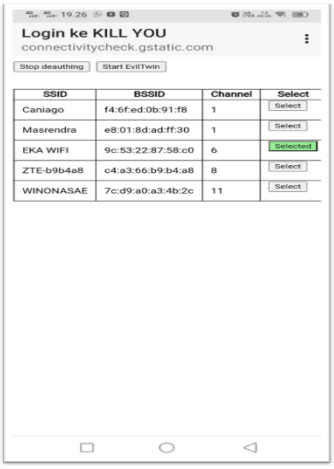
b. Halaman Pilih Target



Gambar 22. Halaman Pilih Target

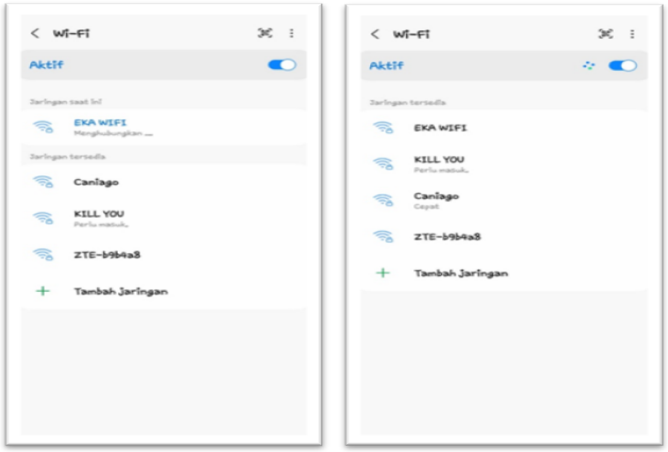
OKTAL : OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 4, April 2024
ISSN 2828-2442 (media online
Hal 885-899

c. Memulai Penetration Testing Dengan Metode Deauther



Gambar 23. *Penetration Testing* Dengan Metode *Deauther*

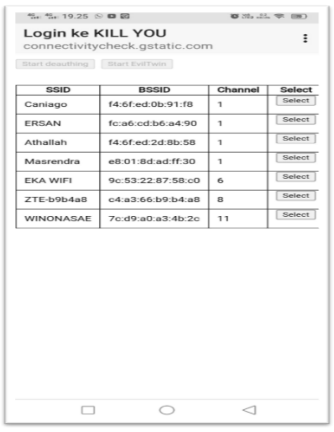
d. Hasil *Penetration Testing Dengan Metode Deauther*



Gambar 24. Hasil *Penetration Testing* Dengan Metode *Deauther*

4.3.2 Implementasi Pengujian Metode Evil Twin

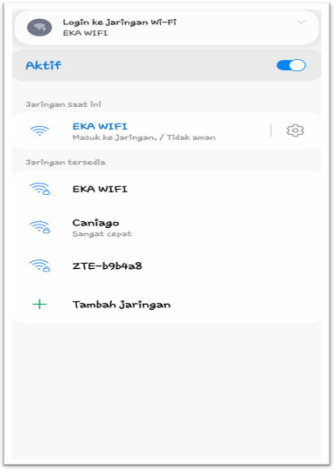
a. Halaman Utama



Gambar 25. Halama Utama

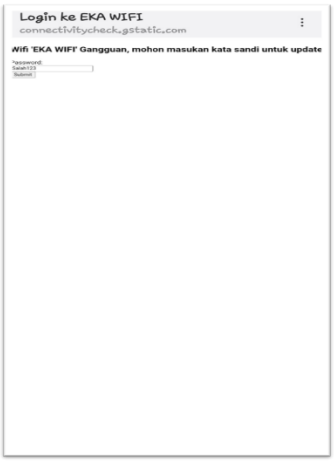
OKTAL : OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 4, April 2024
ISSN 2828-2442 (media online
Hal 885-899

b. Tampilan Wifi Tiruan



Gambar 26. Tampilan Wifi Tiruan

c. Tampilan Utama WiFi Palsu



Gambar 27. Tampilan Utama WiFi Palsu

d. Tampilan Input *Password*

Gambar 28. Tampilan *Input Password*

OKTAL : OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 4, April 2024
ISSN 2828-2442 (media online
Hal 885-899

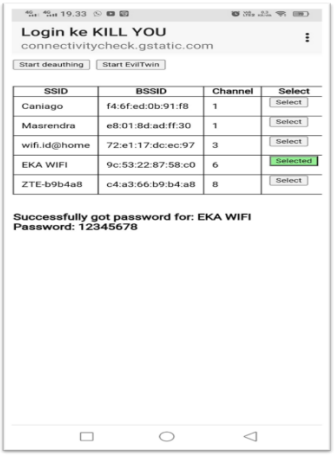
e. Tampilan *Password* salah

Gambar 29. Tampilan *Password* Salah

f. Tampilan *Password* benar

Gambar 30. Tampilan *Password* Benar

g. Hasil dari *Evil Twin*

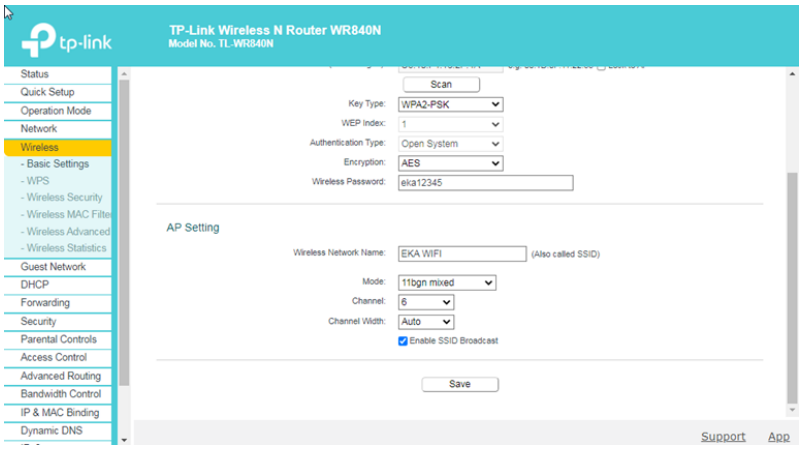


Gambar 31. Tampilan Hasil dari Evil Twin

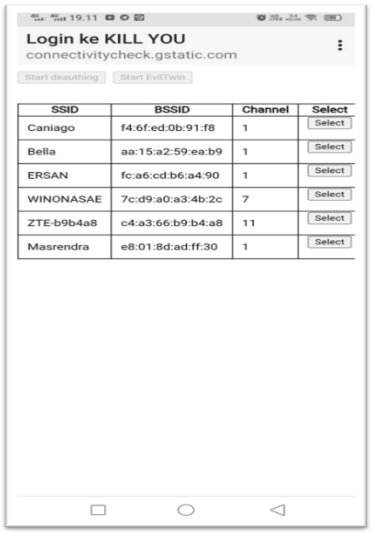
OKTAL : OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 4, April 2024
ISSN 2828-2442 (media online
Hal 885-899

4.3.3 Implementasi Pengamanan

a. Implementasi pengamanan TP- LINK WR840N



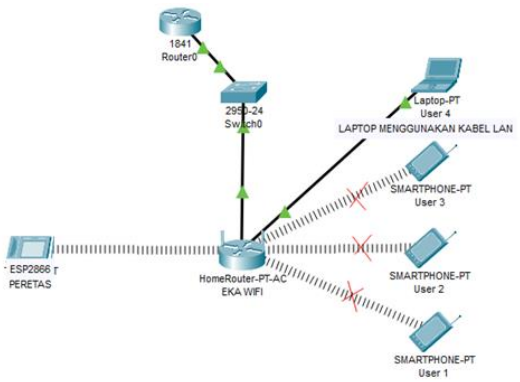
Gambar 32. Setting Di Menu Disable



Gambar 33. Broadcast SSID Tidak Terbaca

4.4 Kasus dan Hasil Pengujian

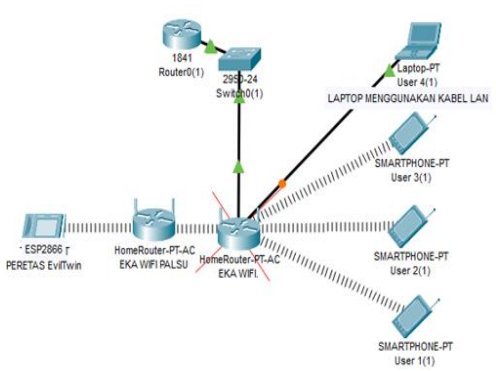
4.4.1 Kasus Pengujian *Deauther*



Gambar 34. Kasus Pengujian *Deauther*

OKTAL : OKTAL : Jurnal Ilmu Komputer dan Science
Volume 3, No. 4, April 2024
ISSN 2828-2442 (media online
Hal 885-899

4.4.2 Kasus Pengujian *Evil Twin*



Gambar 35. Kasus Pengujian *Evil Twin*

4.4.3 Hasil Pengujian Dengan Metode *Deauther* Dan *Evil twin*

Penelitian telah dilakukan dengan menggunakan metode *Deauther* dan *Evil Twin* 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 *Evil Twin* dapat membuat perangkat terhubung ke jaringan palsu yang dikendalikan oleh penyerang.

5. KESIMPULAN

Kesimpulan yang didapatkan pada penelitian ini adalah *Deauther* maupun *Evil Twin* merupakan teknik yang digunakan oleh peretas untuk melakukan serangan terhadap jaringan WiFi. Oleh karena itu, sangat penting bagi pengguna jaringan WiFi untuk menjaga keamanannya dengan menggunakan teknologi keamanan yang tepat, seperti penggunaan kata sandi yang kuat dan enkripsi data. Selain itu, pengguna jaringan juga harus selalu berhati-hati ketika terhubung ke jaringan WiFi publik atau yang tidak dikenal.

REFERENCES

Sitompu, Hamonangan, Ryan, Daniel, Harmaja, Jaya, Okta, Indra, Evta. (2021). Perancangan Pengembangan Desain Arsitektur Jaringan Menggunakan Metode Ppdioo. *JUSIKOM PRIMA* (*Jurnal Sistem Informasi dan Ilmu Komputer Prima*), Vol. 4 No. 2, Februari 2021, E-ISSN : 2580-2879.

Kurniawan, Adi, Turkhamun. (2020). Analisa Keamanan Jaringan Wifi Terhadap Serangan Packet Sniffing. *Jurnal Ilmiah Fakultas Teknik LIMIT'S,* Vol.16 No 2 September 2020, ISSN : 0216-1184.

Setyawan, Okki , Firizkiansah, Angge , Nuryanto, Ahmad. (2021). Klasifikasi Tingkat Keparahan Serangan Jaringan Komputer Dengan Metode Machine Learning. *Journal of Information System, Informatics and Computing*, Vol.5 No.1, Juni 2021, e-ISSN : 2597-3673.

Alfianto, Rizal, Dikky, Sutanto, Yudi. (2022). Analisis Perbandingan Quality of Service (QoS) Firmware Original TL-WR 840N Dengan Firmware Openwrt Berbasis Open Source di Kos Larissa. *Jurnal Teknologi Informasi*, Vol. XVII Nomor 3 November 2022, ISSN: 1907-2430.

Hidayatulloh, Syarif, Saptadiaji, Desky. (2021). Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP). *Jurnal Algoritma*, Vol. 19; No. 1; 2021; Hal 77-86, E-ISSN:2302-7339.

Ismail, Wahyu, Rizky, Pramudita, Rully. (2020). Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT. Puma Makmur Aneka Engineering Bekasi. *Jurnal Mahasiswa Bina Insani*, Vol. 5, No.1, Agustus 2020, 53 – 62, ISSN: 2528-6919.