ANALISIS POLA SOSIAL *ENGINEERING* MENGGUNAKAN TEKNIK *WIFI DEAUTHER* DAN *EVIL TWIN*

Ika Mei Lina[1], Gilang Ryan Fernandes[2]
[1,2]Program Studi Teknik Informatika, Fakultas Teknik dan Ilmu Komputer
Universitas Indraprasta PGRI
Jalan Raya Tengah No. 80, Kelurahan Gedong, Pasar Rebo, Jakarta Timur
ikameilina.24@gmail.com[1], gilang.fernandes@gmail.com[2]

Abstrak

Pada saat ini, WiFi sudah banyak dipasang tidak hanya di lingkungan perkantoran atau pusat perbelanjaan, tetapi juga di perumahan-perumahan sudah banyak terpasang jaringan WiFi. Semakin maraknya minat menggunakan WiFi, semakin banyak pula orang yang tertarik untuk mencari celah keamanan. Hanya dengan memberikan password pada jaringan WiFi, bukan berarti WiFi yang sudah terpasang benar-benar aman. Pada penelitian ini, peneliti melakukan analisis rekayasa sosial dengan menggunakan dua metode, yaitu WiFi deauther dan evil twin untuk menguji kerentanan keamanan WiFi. Deauther bekerja dengan cara memutus jaringan komunikasi elektronik. Sedangkan evil twin adalah penyerangan jaringan dengan meniru teknik access point yang asli. Tujuan dari penelitian ini adalah agar masyarakat lebih memahami bahaya rekayasa sosial dan mampu mengantisipasinya. Dari pengujian yang telah dilakukan, didapatkan hasil bahwa kedua cara yang digunakan terbukti dapat meretas jaringan WiFi yang dituju.

Kata Kunci : WiFi, Social Engineering, Deauther, Evil Twin, Hacking

Abstract

Nowadays, WiFi has been widely installed not only in office environments or shopping centers, but also in many homes that have a WiFi network installed. The more widespread interest in using WiFi, the more people are interested in looking for security holes. Just by giving a password on the WiFi network, it doesn't mean that the WiFi that has been installed is really safe. In this study, researchers conducted a social engineering analysis using two methods, namely WiFi deauther and evil twin to test WiFi security vulnerabilities. Deauther works by breaking the electronic communication network, while evil twin is a network attack by imitating the original access point technique. The purpose of this research is to make the public better understand the dangers of social engineering and be able to anticipate them. From the tests that have been carried out, the results show that the two methods used are proven to be able to hack the targeted WiFi network.

***Keyword** : WiFi, Social Engineering, Deauther, Evil Twin, Hacking*

PENDAHULUAN

Saat ini internet sudah menjadi kebutuhan sehari-hari yang tidak bisa dipisahkan dari kehidupan manusia. Internet sangat memudahkan kita untuk berselancar di dunia maya, baik untuk mencari informasi, membaca artikel, mengunduh dan mengunggah berbagai file, bermain media sosial, dan banyak hal lainnya. Istilah internet sendiri diadaptasi dari bahasa latin yaitu inter yang berarti "antara". Internet adalah dunia maya yang menghubungkan miliaran komputer di dunia melalui jalur telekomunikasi seperti telepon, radio link, satelit dan sebagainya dengan menggunakan protokol TCP/IP [1]. Pada umumnya internet terhubung dengan router dan terhubung dengan perangkat elektronik seperti komputer atau laptop dengan menggunakan kabel LAN. Namun seiring berjalannya waktu, teknologi juga semakin canggih. Bahkan untuk terhubung ke jaringan internet. Kita tidak perlu lagi menggunakan kabel, melainkan bisa menggunakan jaringan WiFi (Wireless Fidelity). WiFi adalah protokol jaringan tanpa kabel yang digunakan perangkat komputer untuk terhubung ke internet dengan menggunakan media transmisi frekuensi dan transmisi radio sebagai pengganti kabel berdasarkan standar protokol jaringan IEEE 802.11 [2].

Jaringan WiFi sudah banyak dipasang tidak hanya di lingkungan perkantoran atau pusat perbelanjaan. Banyak provider berlomba-lomba menawarkan produk WiFi rumahan untuk pengguna di perumahan dalam skala yang lebih kecil. Sehingga semakin banyak rumah yang sudah terpasang jaringan WiFi. Perangkat elektronik yang ingin terhubung ke jaringan WiFi dapat diakses dengan

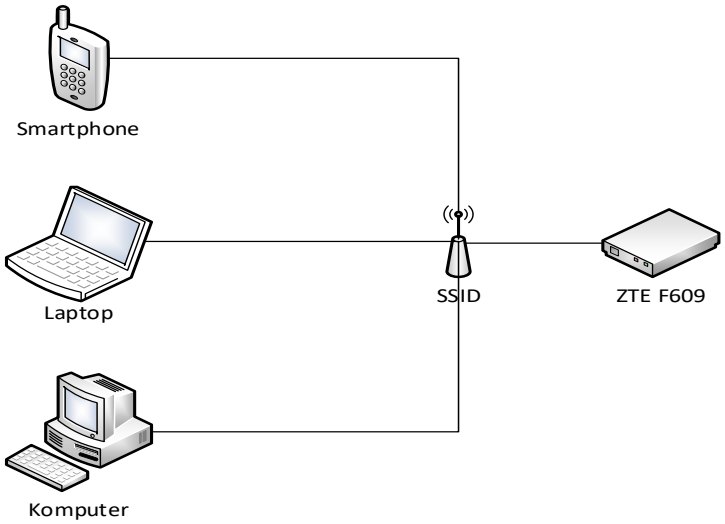
memilih SSID (Service Set Identifier) dan memasukkan password WiFi yang sudah diatur sebelumnya. Namun, hanya dengan memberikan password pada jaringan WiFi, bukan berarti WiFi yang telah terpasang benar-benar aman. Karena ada banyak cara yang bisa disalahgunakan untuk mencuri password jaringan WiFi secara diam-diam. Hal ini didukung oleh pendapat Josua M. Sinambela yang mengatakan bahwa perkembangan teknologi WiFi berkembang sangat pesat sesuai dengan kebutuhan sistem informasi yang mobile, namun jaringan WiFi ini memiliki kelemahan yang lebih banyak dibandingkan jaringan kabel [3]. Kelemahan WiFi secara umum terbagi menjadi dua, yaitu kelemahan pada konfigurasi dan kelemahan pada enkripsi yang digunakan [4].
Dalam kehidupan sehari-hari, WiFi tidak hanya digunakan untuk browsing saja, tetapi juga bisa digunakan untuk sharing file, printer dan lain-lain. Sehingga ketika seseorang yang tidak dikenal memasuki jaringan WiFi yang sama tanpa disadari dapat membahayakan privasi pemilik jaringan WiFi dan file penting yang dimilikinya. Oleh karena itu, peneliti melakukan penelitian tentang metode deauther dan evil twin pada jaringan WiFi dengan tujuan agar masyarakat dapat lebih waspada terhadap kejahatan dunia maya yang dapat merugikan pemilik jaringan WiFi tersebut.

METODE PENELITIAN

Metode yang peneliti gunakan untuk menganalisis pola *social engineering* adalah WiFi *deauther* dan *evil twin* menggunakan program ESP8266. ESP8266 sendiri merupakan *chip* interkoneksi yang dibuat untuk menghubungkan *mikrokontroler* ke internet melalui WiFi sehingga dapat digunakan sebagai *host* atau klien WiFi. Kekuatan pemrosesan dan penyimpanan ESP8266 memungkinkannya untuk diimplementasikan dengan mudah pada sensor dan aplikasi perangkat khusus lainnya. Selain itu, tingkat integrasi ESP8266 sangat tinggi sehingga meminimalkan kebutuhan sirkuit eksternal [5].
Social engineering adalah teknik untuk mendapatkan data dan informasi dengan memanfaatkan kelemahan manusia [6]. Salah satu teknik yang digunakan *hacker* dalam *social engineering* adalah *fake login*, dimana *hacker* akan menggiring korban untuk terjebak dalam *login trap* yang telah dibuat oleh *hacker* sehingga *hacker* mendapatkan data dan informasi korban di dalam *log* miliknya. *Fake login* adalah halaman *login* palsu yang sama persis dengan aslinya dengan tujuan untuk menangkap *username* dan *password* target [7].

Topologi Jaringan

Topologi jaringan adalah cara menghubungkan beberapa perangkat komputer dan menghasilkan jaringan komputer yang saling berhubungan [8]. Berikut adalah perancangan jaringan internet menggunakan modem ZTE F609.



Gambar 1. Topologi WiFi

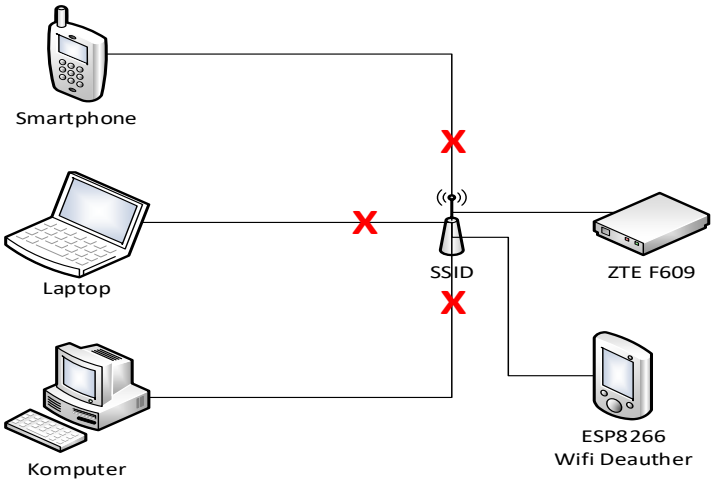
Gambar di atas menunjukkan desain jaringan internet normal menggunakan WiFi dengan perangkat modem ZTE F609. Modem tersebut memiliki spesifikasi *wireless* IEEE 802.11b/g/n dan

menggunakan *security* WPA/WPA2 yang terhubung dengan beberapa perangkat komunikasi seperti *smartphone*, laptop, dan komputer.

Topologi Wifi Deauther

Deauther bekerja dengan memutus jaringan komunikasi elektronik dan menutupinya dengan sinyal baru dengan frekuensi yang sama dengan pemancar aslinya tetapi dengan energi yang lebih tinggi, sehingga penerima hanya akan mendeteksi sinyal baru [9]. Menurut penulis, *deauther attack* digunakan untuk memutus perangkat jaringan WiFi dengan memanfaatkan celah keamanan pada standar WiFi 802.11 [10].

Berikut adalah cara kerja WiFi *Deauther* menggunakan ESP8266 :



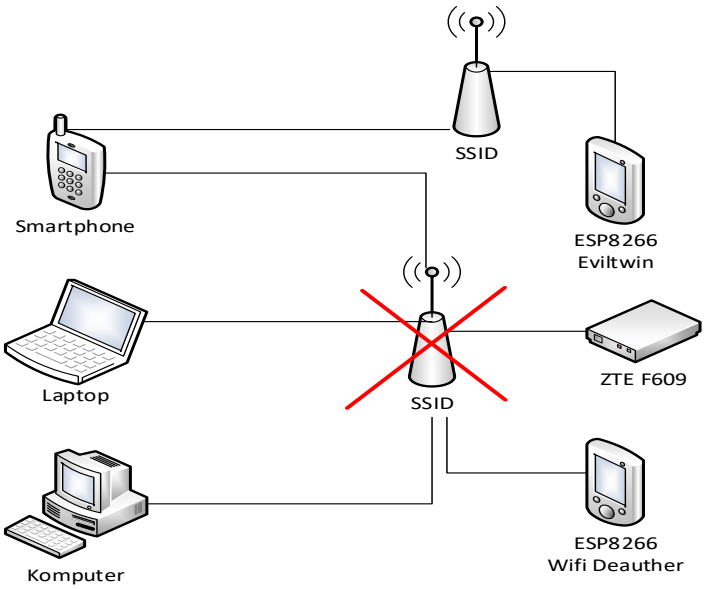
Gambar 2. Topologi WiFi Deauther

Gambar 2 menunjukkan cara kerja WiFi *deauther* dimana penyerang mencoba memutus jaringan koneksi WiFi pada semua perangkat yang terhubung menggunakan ESP8266. Perangkat telah diprogram dengan WiFi *deauther* sebelumnya. Efek dari serangan ini adalah setiap perangkat yang ingin terhubung ke WiFi akan ditolak atau terputus secara paksa.

Topologi *Evil Twin*

Evil twin adalah serangan jaringan menggunakan teknik *man-in-the-middle* (MITM). Teknik ini memungkinkan penyerang mengarahkan korban ke halaman *login* palsu melalui SSID yang digandakan. *Evil twin* adalah serangan yang dapat mengatur *access point* sebagai perangkat yang memiliki kemampuan meniru SSID, MAC *Address* dan trafik pada *access point* asli [11].

Berikut cara kerja *Evil Twin* menggunakan ESP8266:



Gambar 3. Topologi Evil Twin

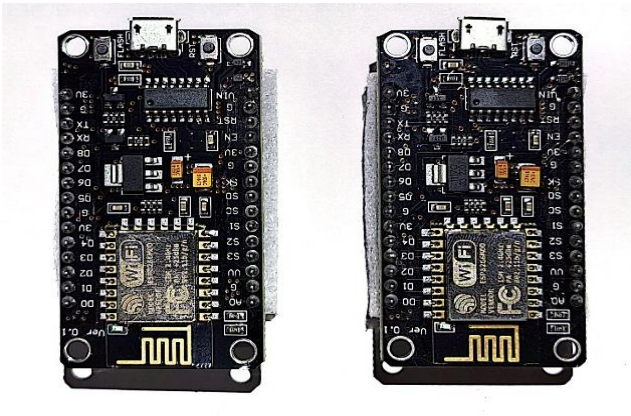
Pada Gambar 3 terlihat bahwa semua perangkat tidak dapat lagi terhubung ke jaringan WiFi yang tersedia sebelumnya. Pada saat yang sama, ESP8266 yang diprogram dengan *evil twin* menggandakan SSID, dimana korban akan bingung dengan adanya dua SSID yang muncul bersamaan dan secara tidak sengaja memilih WiFi yang digandakan.

HASIL DAN PEMBAHASAN

Implementasi dilakukan pada jaringan WiFi yang terhubung secara normal. Namun peneliti akan menguji keamanan WiFi tersebut menggunakan teknik WiFi *deauther* dan *evil twin*. Tindakan ini peneliti lakukan guna memberikan pemahaman tentang antisipasi keamanan jaringan WiFi.

Implementasi Dan Testing

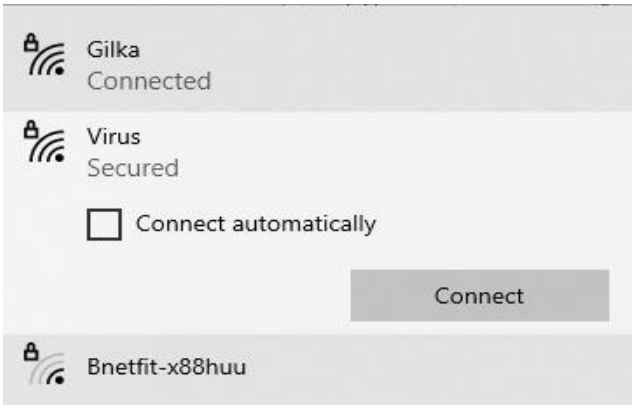
Langkah pertama yang harus dilakukan adalah menyalakan kedua ESP8266 yang sudah diprogram, dimana kedua perangkat tersebut memiliki fungsinya masing-masing.



Gambar 4. ESP8266

Pada gambar diatas ada dua buah ESP8266 yang sudah diprogram dan akan diaktifkan. Peneliti menggunakan dua buah ESP8266 karena dianggap lebih efisien dan stabil dalam hal meretas jaringan WiFi.

Ketika *deauther* WiFi ESP8266 diaktifkan, akan muncul SSID baru bernama Virus, seperti gambar di bawah ini :

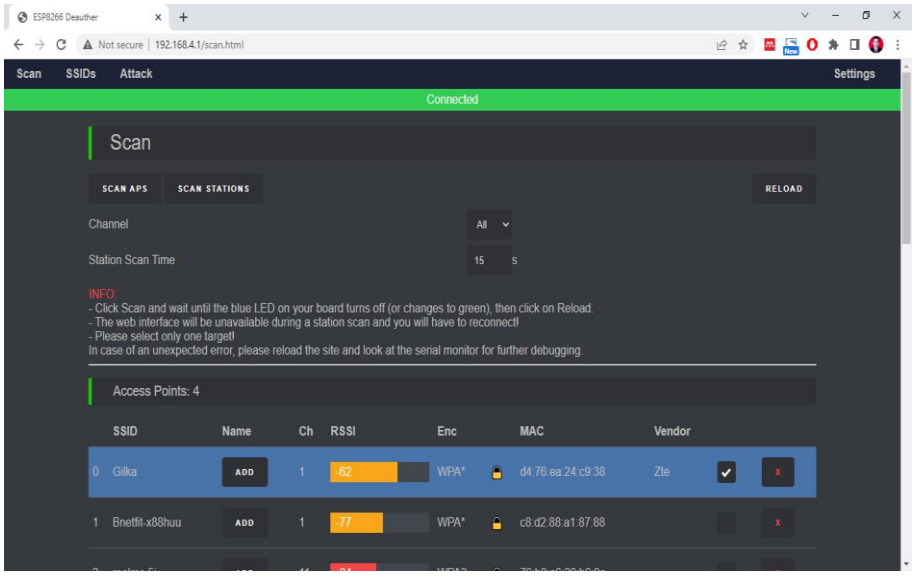


Gambar 5. SSID Network

Agar bisa menyerang, terlebih dahulu kita harus terhubung dengan Virus SSID yang sudah diaktifkan sebelumnya. Serangan akan dilakukan melalui *interface deauther* pada ESP8266.

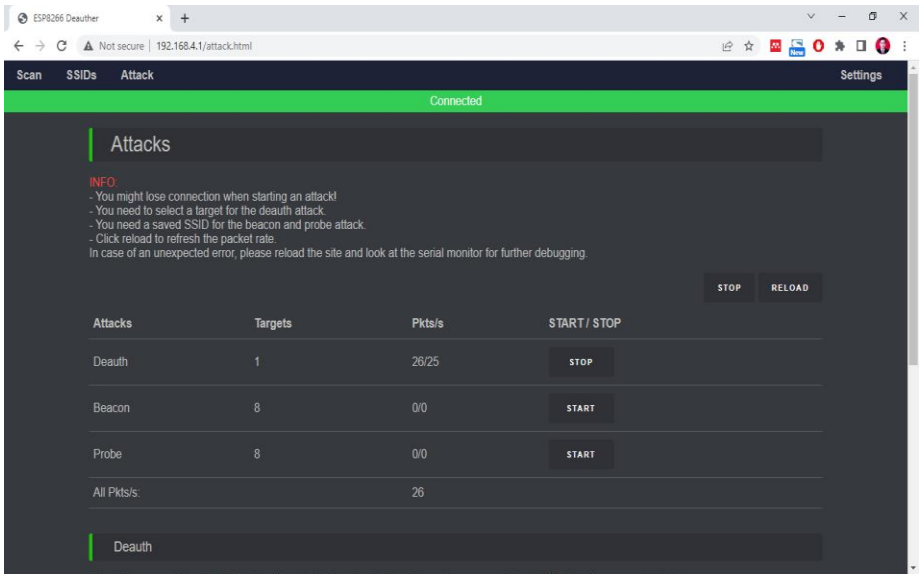
Teknik Serangan

Setelah berhasil terkoneksi dengan SSID Virus maka *interface deauther* dapat dibuka. Langkah selanjutnya ketikkan alamat IP 192.168.4.1 pada *browser* sehingga akan muncul tampilan seperti berikut :



Gambar 6. Interface Deauther

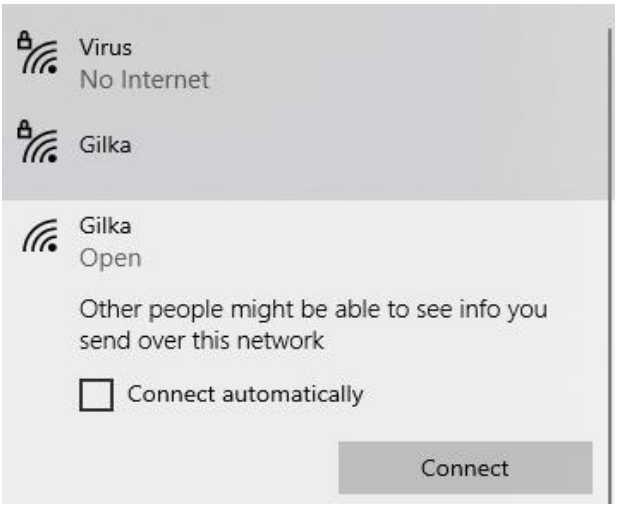
Pada bagian atas *interface* pada Gambar 6 terdapat tiga menu yaitu *Scan*, SSIDs dan *Attack*. Selanjutnya kita masuk ke bagian *access point* yang terdapat pada menu *scan*. Dengan mencentang SSID yang diinginkan sebagai target, SSID akan terputus. Pada gambar terlihat bahwa SSID bernama Gilka dipilih untuk pemutusan koneksi. Jaringan WiFi dengan nama SSID Gilka merupakan jaringan WiFi percobaan yang dimiliki oleh peneliti secara pribadi.



Gambar 7. Menu Attack

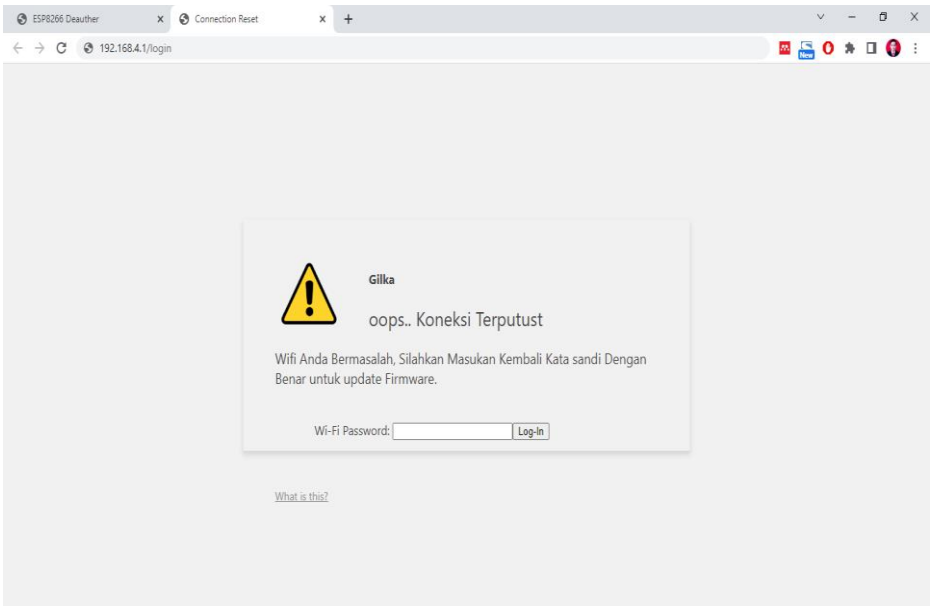
Setelah memilih SSID target yang akan diputus, maka pada menu *attack* akan terlihat bahwa target pada kolom *deauther* berubah menjadi 1 dan paket-paket di samping kolom target berubah setelah mengklik tombol *start.* Dalam kondisi ini, koneksi internet korban terputus dan tidak bisa terhubung kembali.

Langkah selanjutnya melakukan setting pada *evil twin* dimana dalam hal ini peneliti akan menggandakan SSID target dengan tujuan agar target menjadi bingung dan panik sehingga memilih SSID baru yang merupakan hasil duplikasi dari *evil twin* teknik. Berikut tampilan SSID yang telah di duplikasi :



Gambar 8. Duplikasi SSID

Pada gambar di atas terlihat ada dua SSID dengan nama Gilka. Dimana kondisi SSID target semula tidak bisa lagi terkoneksi ke semua perangkat. Kemudian muncul SSID palsu dengan nama yang sama yang dapat terhubung ke jaringan WiFi.



Gambar 9. Fake Login

Ketika target terpancing untuk terhubung dengan SSID palsu, maka target akan diarahkan ke halaman *login* palsu untuk memasukkan kembali *password* WiFi dengan tujuan mengupdate *firmware* pada perangkat modem. Setelah target memasukkan *password* dengan benar maka perangkat ESP8266 yang telah diprogram dengan WiFi *deauther* dan *evil twin* akan otomatis berhenti sehingga target dapat menggunakan WiFi dan internet kembali. Di sisi lain, *hacker* yang memanfaatkan kepanikan target berhasil mendapatkan *password* WiFi yang tersimpan di *evil twin logs.*

Penjelasan di atas menunjukkan cara kerja rekayasa sosial dengan memanfaatkan kepanikan target dan menggiring target untuk terjebak dalam *login* palsu yang telah disiapkan oleh *hacker*.

SIMPULAN

Dari implementasi dan pengujian di atas, peneliti dapat menyimpulkan bahwa jaringan WiFi yang sudah memiliki *password* masih rentan terhadap serangan rekayasa sosial. Teknik WiFi *deauther* dan *evil twin* yang digunakan terbukti menjadi ancaman bagi pemilik jaringan WiFi yang tidak mengetahui keamanan jaringan.
Sebagai langkah antisipatif terhadap kedua teknik rekayasa sosial yang telah dijelaskan, peneliti memberikan saran kepada pengguna perangkat WiFi untuk mengganti nama SSID secara berkala dan melakukan jaringan tersembunyi agar SSID tidak dapat dilihat oleh pengguna lain. Sebaiknya gunakan antivirus dan anti netcut atau anti ARP pada perangkat yang terhubung dengan jaringan WiFi. Gunakan juga modem atau *router* yang mendukung WiFi 802.11w-2009. Yang terpenting untuk menghindari rekayasa sosial di atas adalah jangan panik dan terburu-buru mengganti koneksi pada WiFi yang memiliki SSID dengan nama yang sama.

DAFTAR PUSTAKA

[1] A. G. Gani, “Pengenalan Teknologi Internet Serta Dampaknya,” J. Sist. Inf. Univ. Suryadarma, vol. 2, no. 2, 2014, doi: 10.35968/jsi.v2i2.49.
[2] H. Nugroho and S. A. Siagian, “Analisis Bandwidth Jaringan Wifi,” ICT Penelit. dan Penerapan Teknol., vol. 4, no. 6, pp. 35–43, 2013.
[3] J. M. Sinambela, “Keamanan Wireless LAN (Wifi),” Gadjahmada.Edu, no. April, p. 5, 2007.
[4] Y. Yanti, S. Pengajar, P. Studi, and T. Informatika, “Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WiFi,” vol. III, no. 1, pp. 248–254, 2018.
[5] M. R. Hidayat, C. Christiono, and B. S. Sapudin, “PERANCANGAN SISTEM KEAMANAN RUMAH BERBASIS IoT DENGAN NodeMCU ESP8266 MENGGUNAKAN SENSOR PIR HC-

SR501 DAN SENSOR SMOKE DETECTOR," Kilat, vol. 7, no. 2, pp. 139–148, 2018, doi: 10.33322/kilat.v7i2.357.

[6] D. I. Junaedi, "Antisipasi Dampak Social Engineering Pada Bisnis Perbankan," Infoman's, vol. 11, no. 1, pp. 1–10, 2017, doi: 10.33481/infomans.v11i1.13.

[7] D. Irawan, "Jurnal Ilmu Komputer & Informatika MENCURI INFORMASI PENTING DENGAN MENGAMBIL ALIH AKUN FACEBOOK DENGAN METODE PHISING Jurnal Ilmu Komputer & Informatika," vol. 1, no. 1, pp. 43–46, 2020.

[8] U. Smk, K. X. Teknik, and K. Dan, "PENGEMBANGAN MULTIMEDIA TUTORIAL TOPOLOGI JARINGAN UNTUK SMK KELAS X TEKNIK KOMPUTER DAN JARINGAN Muchammad Azwar Anas, Yerry Soepriyanto, Susilaningsih," pp. 307–314, 2013.

[9] R. Agustiningsih, D. Suryadi, and Dasril, "Rancang Bangun Alat Pemblocking Sinyal (Jammer) Pada Sistem Telekomunikasi Jaringan Seluler Global System For Mobile (GSM) Di Area Bebas Sinyal GSM," Jteuntan, vol. 1, no. 1, pp. 946–952, 2018, [Online]. Available: http://jurnal.untan.ac.id/index.php/jteuntan/article/view/25220

[10] SpacehuhnTech, "GitHub - SpacehuhnTech/esp8266_deauther: Affordable WiFi hacking platform for testing and learning." https://github.com/SpacehuhnTech/esp8266_deauther (accessed Oct. 30, 2022).

[11] R. Renaldi, U. M. Buana, M. Sadikin, and U. M. Buana, "Analisa dan Pengujian Serangan Evil Twin pada Jaringan berbasis Wireless Analisa dan Pengujian Serangan Evil Twin pada Jaringan berbasis Wireless dengan Keamanan WPA2-PSK," no. September, 2019.