(2024), 2 (11): 193-214 Scientica 3021-8209
Jurnal Ilmiah Sain dan Teknologi

PENGUJIAN SERANGAN *EVIL TWIN* ESP8266 PADA *WIRELESS NETWORKING* DENGAN METODE *PENETRATION TESTING* (STUDI KASUS: SEKOLAH TINGGI TEKNOLOGI WASTUKANCANA)

Muhammad Sigit [1], Dayan Singasatia, S.Kom, M.Kom [2], Imay Kurniawan, M.Kom. [3]
Program Studi Teknik Informatika
Sekolah Tinggi Teknologi Wastukancana
Purwakarta
rd.muhsigit02@gmail.com

Abstrak (Indonesia)
Penelitian ini meneliti risiko serangan *Evil Twin* pada jaringan nirkabel di Sekolah Tinggi Teknologi Wastukancana (STT Wastukancana) menggunakan metode *Penetration Testing*. Serangan *Evil Twin* melibatkan pembuatan titik akses palsu yang meniru titik akses sah, memungkinkan penyerang untuk mengakses data sensitif pengguna. Tujuan penelitian ini adalah mengevaluasi kemungkinan serangan *Evil Twin* dan mengidentifikasi kerentanan jaringan, dengan tujuan memberikan rekomendasi pencegahan yang tepat. Hasil penelitian menunjukkan bahwa serangan *Deauthentification* berhasil dilakukan di dua lokasi: LAB_IOT dengan password "IOTJAR123" dan AUDITORIUM 1 dengan *password* "STTWASTU1". Pengguna terjebak pada titik akses palsu, menunjukkan kerentanan jaringan nirkabel. Penelitian ini diharapkan dapat meningkatkan pemahaman tentang serangan *Evil Twin* dan mengoptimalkan keamanan jaringan nirkabel, memastikan aktivitas pendidikan dan administratif berjalan lancar tanpa mengorbankan integritas data.

Sejarah Artikel
Submitted: 16 Juli 2024
Accepted: 19 Juli 2024
Published: 26 Juli 2024

Kata Kunci
Pengujian, keamanan jaringan, jaringan nirkabel, *Evil Twin*, *penetration testing*

Abstract (English)
This study investigates the risk of Evil Twin attacks on wireless networks at the Sekolah Tinggi Teknologi Wastukancana (STT Wastukancana) using Penetration Testing methods. The Evil Twin attack involves creating a fake access point that mimics a legitimate access point, allowing attackers to access users' sensitive data. The aim of this research is to evaluate the potential for Evil Twin attacks and identify vulnerabilities in the network, with the goal of providing appropriate preventive recommendations. The results show that Deauthentication attacks were successfully executed at two locations: LAB_IOT with the password "IOTJAR123" and AUDITORIUM 1 with the password "STTWASTU1". Users were trapped on the fake access point, highlighting vulnerabilities in the wireless network. This research is expected to enhance understanding of Evil Twin attacks and optimize wireless network security, ensuring that educational and administrative activities continue smoothly without compromising data integrity.

Article History
Submitted: 16 Juli 2024
Accepted: 19 Juli 2024
Published: 26 Juli 2024

Key Words
Testing, network security, wireless networks, Evil Twin, penetration testing

Latar Belakang Masalah

Dalam era digital saat ini, teknologi nirkabel atau *wireless* telah menjadi bagian integral dari kehidupan sehari-hari. Dari rumah tangga hingga perusahaan besar, penggunaan jaringan nirkabel semakin meningkat karena fleksibilitas dan kenyamanan yang ditawarkan. Penggunaan jaringan nirkabel telah menjadi semakin meluas dalam berbagai aspek kehidupan modern. Di Sekolah Tinggi Teknologi Wastukancana, kemudahan akses internet yang diberikan oleh jaringan nirkabel memungkinkan fleksibilitas dan mobilitas bagi pengguna, baik itu mahasiswa, dosen, maupun staf administrasi, dalam mengakses sumber daya informasi yang diperlukan. Namun, bersamaan dengan manfaatnya, keberadaan jaringan nirkabel juga membawa risiko keamanan yang signifikan.

Menurut Priyambodo (2015:5) Wireless merupakan standar dari jaringan tanpa kabel atau yang dikenal dengan nama Wireless Networking dengan fungsi untuk menyempurnaan

komponenkomponen pada jaringan internet agar teroneksikan atau agar terhubung dengan internet dengan mudah dan tanpa ribet.(Hafiz & Kurnia, 2021)

Salah satu bentuk ancaman utama dalam keamanan jaringan nirkabel adalah serangan Evil Twin. Serangan ini melibatkan pembuatan titik akses nirkabel palsu yang meniru titik akses sah dengan menggunakan nama dan parameter jaringan yang sama. Penyerang menggunakan metode ini untuk menipu pengguna agar terhubung ke jaringan palsu tersebut. Setelah pengguna terhubung, penyerang dapat dengan mudah memantau atau mencuri data sensitif yang ditransmisikan. Dengan kemajuan teknologi yang terus berkembang, serangan Evil Twin menjadi semakin canggih dan sulit dideteksi, sehingga meningkatkan risiko terhadap jaringan nirkabel. Sebagai contoh, di Sekolah Tinggi Teknologi Wastukancana (STT Wastukancana), pernah terjadi insiden di mana beberapa mahasiswa yang terhubung ke jaringan kampus secara tiba tiba jaringan tersebut tidak dapat diakses sehingga mahasiswa tanpa sadar terhubung ke jaringan palsu yang dibuat oleh penyerang, yang mengakibatkan penyerang memiliki password jaringan tersebut yang berakibat data pribadi dapat dieksploitasi. Baloch (Baloch, 2015 : 340) mengatakan bahwa, *Evil Twin* Attack adalah jenis serangan (social engineering) yang sangat populer terhadap klien. Gagasan dibalik serangan ini adalah untuk menciptakan jalur akses dengan nama yang mirip dengan apa yang menjadi korban dan menyebabkan penolakan layanan kejalur akses point semula (Denial of Service to The Original Access Point). Ini akan membuat korban kita terhubung ke akses point palsu kita dengan pemikiran bahwa itu adalah yang asli. Selanjutnya, penyerang juga akan menipu alamat MAC dari interface untuk mencocokkan alamat MAC dari akses point sebenarnya.(Antoni, 2020)
Untuk mengatasi ancaman serangan *Evil Twin* dan menjaga keamanan jaringan nirkabel, penting untuk melakukan pengujian keamanan secara teratur menggunakan metode yang sesuai. Salah satu metode yang umum digunakan dalam pengujian keamanan jaringan adalah metode *Penetration Testing* . Metode ini memungkinkan peneliti atau praktisi keamanan untuk mengevaluasi kelemahan dan kerentanan dalam infrastruktur jaringan nirkabel, serta mengidentifikasi potensi serangan yang mungkin terjadi. Namun, menguji keamanan jaringan nirkabel tidaklah mudah. Lingkungan jaringan yang kompleks dan terus berkembang, serta beragamnya jenis perangkat yang terhubung ke jaringan tersebut, membuat tantangan tersendiri dalam mengidentifikasi dan mengatasi ancaman keamanan. Terlebih lagi, serangan *Evil Twin* dapat muncul tanpa peringatan dan menimbulkan kerugian besar jika tidak ditangani dengan cepat dan tepat.

METODOLOGI PENELITIAN

Dalam penelitian ini, metode yang diusulkan mengadopsi pendekatan analisis kualitatif deskriptif. Melalui serangkaian tahapan yang terinci, termasuk Pengumpulan Data dan Penetration Testing untuk mendapatkan pemahaman yang mendalam tentang kerentanan keamanan dalam jaringan nirkabel.

HASIL DAN PEMBAHASAN

Hasil Pengumpulan Data

Pengumpulan data dalam penelitian ini menggunakan metode kualitatif melibatkan observasi, wawancara, dan studi literatur yang berkaitan dengan pengujian serangan *Evil Twin* adapun berikut ini hasil yang didapat:

Observasi

Dari Dari hasil observasi di STT Wastukancana Purwakarta, ditemukan banyak jaringan nirkabel *Wireless Fidelity* (*Wi-Fi*), baik yang terpasang di lingkungan kampus maupun yang dimiliki oleh mahasiswa. Jaringan *Wi-Fi* ini menggunakan berbagai protokol keamanan, termasuk WEP, WPA, WPA2, dan WPA3. Dalam penelitian ini, fokus dibatasi pada jaringan

Wi-Fi yang menggunakan protokol WPA2 atau WPA3 dengan sistem keamanan berbasis kata sandi, untuk memudahkan pengujian serangan *Evil Twin*. Penelitian ini menargetkan dua jaringan *Wi-Fi* di STT Wastukancana yang menggunakan keamanan WPA2 atau WPA3.

Wawancara

Setelah melakukan observasi, langkah selanjutnya adalah mengumpulkan informasi tentang jaringan nirkabel melalui wawancara. Dari hasil wawancara dengan pihak kampus, staf, dosen, dan mahasiswa di lingkungan STT Wastukancana, ditemukan bahwa *Wi-Fi* yang paling sering digunakan dan banyak terhubung adalah jaringan LABIOT dan AUDITORIUM 1. Kedua jaringan *Wi-Fi* ini menggunakan protokol keamanan WPA2/WPA3, sesuai dengan informasi yang dibutuhkan peneliti untuk melakukan serangan *Evil Twin*.

Studi Literatur

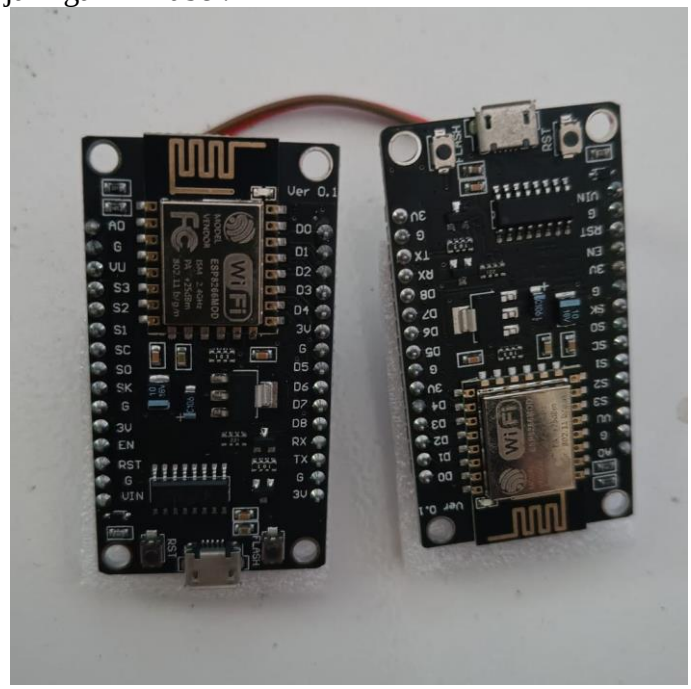
Hasil dari studi literatur yang dilakukan peneliti mencakup pencarian referensi dan informasi mengenai berbagai konsep yang mendekati pengujian, serangan *Evil Twin* serta metode *Penetration Testing*. Referensi ini termasuk buku, jurnal, dan skripsi, yang semuanya digunakan untuk memperkuat dasar penelitian ini.

Pre-engagement (Pra Interaksi)

Dalam tahap Pra Interaksi yang telah dilakukan, mendapatkan kebutuhan yang perlu dipersiapkan untuk ke tahap selanjutnya berupa perangkat. Berikut kebutuhan yang diperlukan dalam melakukan penelitian ini.

Kebutuhan Perangkat Keras dan Lunak

Alat yang pertama, ESP8266 Evil Twin, digunakan untuk menciptakan akses poin palsu yang menyerupai jaringan asli, guna menguji keamanan jaringan nirkabel dengan mencoba memikat pengguna agar terhubung ke akses poin palsu tersebut. ESP8266 Deauthentication digunakan untuk melakukan serangan deauthentication terhadap perangkat yang terhubung ke jaringan WiFi. Dengan menggunakan ESP8266 Deauthentication, peneliti dapat mengirimkan paket deauth ke perangkat target untuk memutus koneksi mereka dari jaringan WiFi, sehingga memudahkan pengujian kerentanan jaringan. Kedua perangkat ini esensial dalam skenario pengujian penetrasi jaringan nirkabel.



gambar 1 ESP8266 Evil Twin

Selanjutnya, Wireless Adapter TP-Link TL-WN722N digunakan untuk scanning jaringan nirkabel. Adapter ini memungkinkan peneliti untuk mendeteksi dan menganalisis berbagai jaringan WiFi yang ada di sekitarnya. Dengan kemampuan antena eksternal berdaya tinggi, adapter ini dapat menangkap sinyal WiFi dari jarak yang lebih jauh, memberikan cakupan yang lebih luas dalam analisis jaringan. Adapter ini juga mendukung mode monitor, yang memungkinkan peneliti untuk menangkap paket data yang dikirimkan melalui jaringan WiFi tanpa harus terhubung ke jaringan tersebut.

Gambar 2 *Wireless Adpter* TP-Link TL-WN722N

Selain perangkat keras, penelitian ini juga memerlukan perangkat lunak khusus. Sistem Operasi Kali Linux adalah sistem operasi yang sangat penting dalam pengujian penetrasi dan keamanan siber. Kali Linux menyediakan berbagai alat keamanan siber dan forensik digital yang komprehensif, yang memudahkan peneliti dalam melakukan berbagai jenis pengujian dan analisis keamanan jaringan.

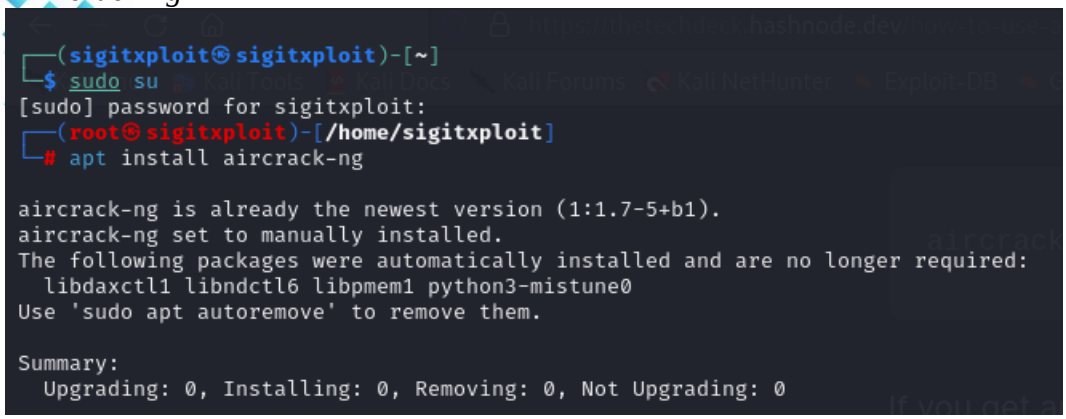
Google Chrome digunakan sebagai peramban web untuk mengakses antarmuka ESP8266 Evil Twin maupun Deauther. Melalui Google Chrome, peneliti dapat mengonfigurasi dan mengendalikan perangkat ini dengan mudah, melakukan serangan simulatif, serta memantau aktivitas jaringan yang sedang diuji.

Perangkat keras dan perangkat lunak ini esensial dalam skenario pengujian penetrasi jaringan nirkabel, membantu peneliti memahami dan mengidentifikasi potensi celah keamanan pada jaringan yang diuji. Dengan menggunakan kombinasi perangkat ini, peneliti dapat menjalankan berbagai jenis pengujian dan serangan simulatif untuk mengevaluasi keamanan jaringan secara menyeluruh, memberikan wawasan yang diperlukan untuk memperkuat pertahanan jaringan.

Instalasi *Tool* di Kali Linux

Dalam sistem operasi Kali Linux, untuk melangkah ke tahap selanjutnya dalam pengujian keamanan jaringan, diperlukan instalasi beberapa perangkat, termasuk tool seperti *Aircrack-ng* dan *Wifite*, serta pengaturan driver untuk *wireless adapter* TP-Link TL-WN722N agar menunjang yang diperlukan.

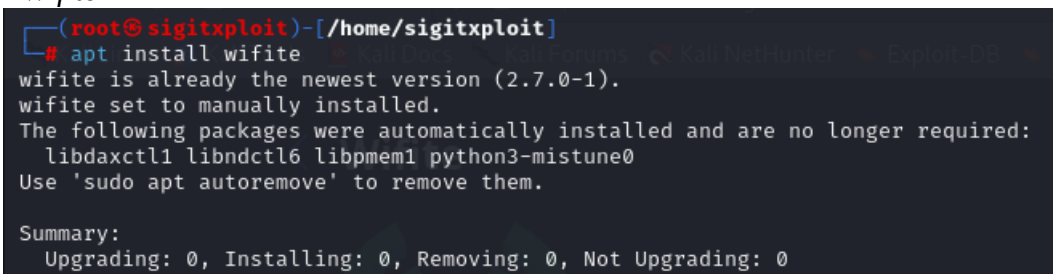
1) *Aircrack-ng*



Gambar 3 Instalasi *Aircrack-ng*

Instalasi *Aircrack-ng* sangat penting untuk mempersiapkan proses pemindaian jaringan nirkabel dengan tujuan mencari target dan mengidentifikasi jaringan yang ada. *Aircrack-ng* menyediakan berbagai alat yang diperlukan untuk memonitor lalu lintas jaringan, menganalisis keamanan protokol seperti WEP dan WPA, serta menjalankan serangan terhadap jaringan *Wi-Fi*. Dengan demikian, Aircrack-ng berperan sebagai perantara yang krusial dalam persiapan untuk pengujian keamanan jaringan nirkabel.

2) *Wifite*

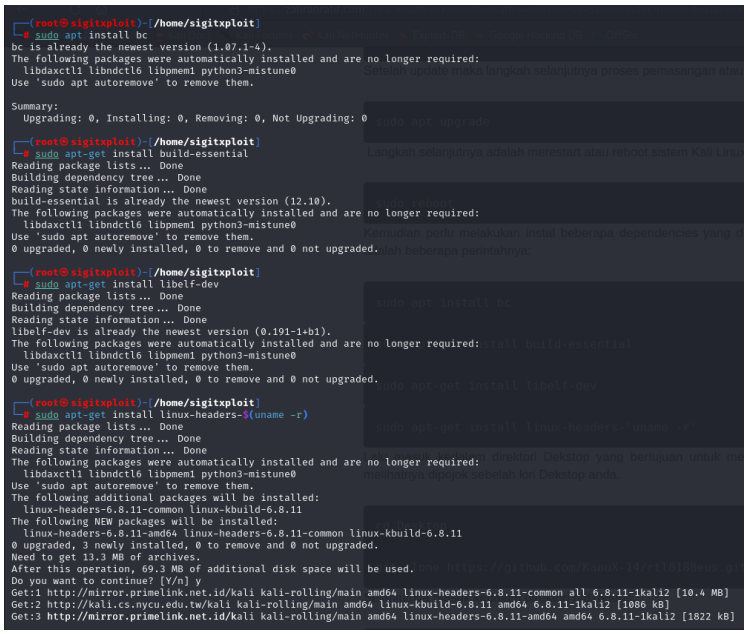


Gambar 4 Instalasi *Wifite*

Wifite perlu diinstal untuk memperkaya informasi terhadap jaringan yang sebelumnya dipindai oleh Aircrack-ng. Alat ini memainkan peran penting dalam mempersiapkan target untuk menjalankan pengujian serangan *Evil Twin*.

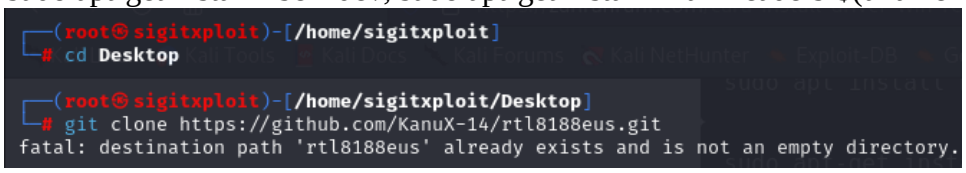
Instalasi *Driver Wi-fi Realtek* RTL8188EUS

Selanjutnya dalam melakukan scanning perlu menggunakan *wireless adapter* TP-Link TL-WN722N agar *wireless adapter* dapat melakukan scanning menggunakan *aircrack-ng* dan *wifite* perlu melakukan instalasi driver terlebih dahulu. *Driver wi-fi realtek* RTL8188EUS sebagai pilihan yang digunakan berikut proses instalasinya.



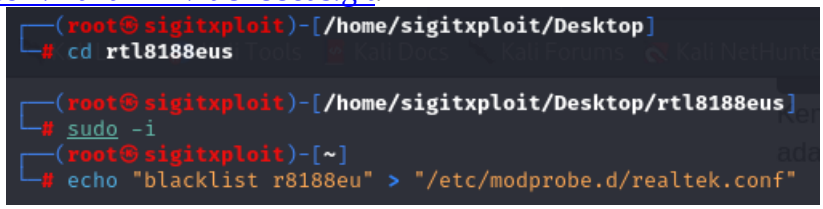
Gambar 5 *Dependencies* yang dibutuhkan

Pertama melakukan instal beberapa *dependencies* yang dibutuhkan agar *driver* dapat berjalan sempurna. Dengan memasukan perintah sudo apt install bc, sudo apt-get install build-essential, sudo apt-get install libelf-dev, sudo apt-get install linux-headers-$(uname -r).



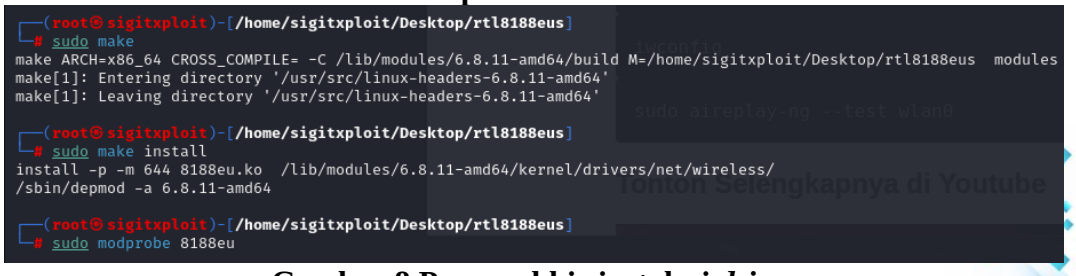
Gambar 6 Mengunduh driver *realtek* RTL8188EUS

Kemudian mengunduh driver *realtek* RTL8188EUS dengan memasukan perintah git clone https://github.com/KanuX-14/rtl8188eus.git.



Gambar 7 Direktori rtl8188eus

Masuk kedalam direktori rtl8188eus dengan memasukan perintah cd rtl8188eus, sudo -I, echo "blacklist r8188eu" >"/etc/modprobe.d/realtek.conf".



Gambar 8 Proses akhir instalasi *driver*

Setelah masuk kedalam direktori *driver* selanjutnya lakukan perintah sudo make, sudo make install dan sudo modprobe 8188eu. Proses instalasi driver telah selesai. Pada akhirnya *wireless adapter* TP-Link TL-WN722N dapat digunakan untuk *scaning* dengan menggunakan *tool aircrack-ng* dan *wifite*.

Konfigurasi Perangkat

Sebelum memulai pemindaian jaringan nirkabel, perlu dilakukan konfigurasi dengan mengubah mode dari "*managed*" menjadi "*monitor*", seperti yang ditunjukkan pada Gambar 9 di bawah ini.

Gambar 8 Konfigurasi

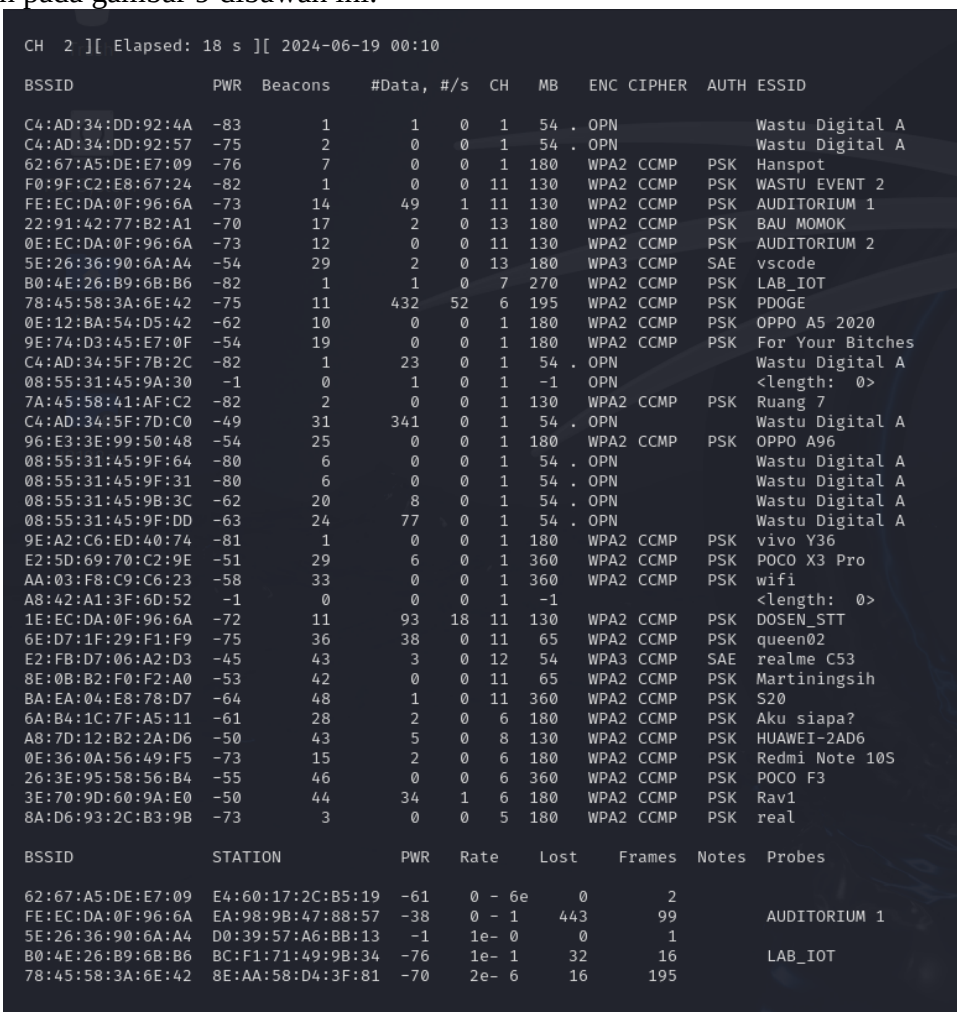
Dengan menjalankan perintah "airmon-ng start wlan0", antarmuka jaringan akan beralih ke mode monitor. Perubahan ini dapat diverifikasi dengan perintah "iwconfig", di mana mode antarmuka yang sebelumnya "*managed*" akan terlihat telah berubah menjadi "*monitor*".

Intelligence Gathering (Pengumpulan Informasi)

Jika sudah memiliki perangkatnya selanjutnya pada tahap pengumpulan informasi melakukan *scanning* jaringan untuk menentukan target yang berpotensi dapat dilakukan pengujian serangan *Evil Twin*.

Scanning Aircrack-ng

Scanning menggunakan *Wireless Adpter* TP-Link TL-WN722N yang sudah dalam mode monitor didalam kali linux. Di kali linux sendiri menggunakan *tool scanning* yang ada seperti aircrack-ng dengan memasukan perintah "airodump-ng wlan0". *output scanning* ditunjukan pada gambar 9 dibawah ini.



```
CH  2 ][ Elapsed: 18 s ][ 2024-06-19 00:10

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

C4:AD:34:DD:92:4A  -83        1        1    0   1   54 . OPN              Wastu Digital A
C4:AD:34:DD:92:57  -75        2        0    0   1   54 . OPN              Wastu Digital A
62:67:A5:DE:E7:09  -76        7        0    0   1  180   WPA2 CCMP   PSK  Hanspot
F0:9F:C2:E8:67:24  -82        1        0    0  11  130   WPA2 CCMP   PSK  WASTU EVENT 2
FE:EC:DA:0F:96:6A  -73       14       49    1  11  130   WPA2 CCMP   PSK  AUDITORIUM 1
22:91:42:77:B2:A1  -70       17        2    0  13  180   WPA2 CCMP   PSK  BAU MOMOK
0E:EC:DA:0F:96:6A  -73       12        0    0  11  130   WPA2 CCMP   PSK  AUDITORIUM 2
5E:26:36:90:6A:A4  -54       29        2    0  13  180   WPA3 CCMP   SAE  vscode
B0:4E:26:B9:6B:B6  -82        1        1    0   7  270   WPA2 CCMP   PSK  LAB_IOT
78:45:58:3A:6E:42  -75       11      432   52   6  195   WPA2 CCMP   PSK  PDOGE
0E:12:BA:54:D5:42  -62       10        0    0   1  180   WPA2 CCMP   PSK  OPPO A5 2020
9E:74:D3:45:E7:0F  -54       19        0    0   1  180   WPA2 CCMP   PSK  For Your Bitches
C4:AD:34:5F:7B:2C  -82        1       23    0   1   54 . OPN              Wastu Digital A
08:55:31:45:9A:30   -1        0        1    0   1   -1   OPN              <length:  0>
7A:45:58:41:AF:C2  -82        2        0    0   1  130   WPA2 CCMP   PSK  Ruang 7
C4:AD:34:5F:7D:C0  -49       31      341    0   1   54 . OPN              Wastu Digital A
96:E3:3E:99:50:48  -54       25        0    0   1  180   WPA2 CCMP   PSK  OPPO A96
08:55:31:45:9F:64  -80        6        0    0   1   54 . OPN              Wastu Digital A
08:55:31:45:9F:31  -80        6        0    0   1   54 . OPN              Wastu Digital A
08:55:31:45:9B:3C  -62       20        8    0   1   54 . OPN              Wastu Digital A
08:55:31:45:9F:DD  -63       24       77    0   1   54 . OPN              Wastu Digital A
9E:A2:C6:ED:40:74  -81        1        0    0   1  180   WPA2 CCMP   PSK  vivo Y36
E2:5D:69:70:C2:9E  -51       29        6    0   1  360   WPA2 CCMP   PSK  POCO X3 Pro
AA:03:F8:C9:C6:23  -58       33        0    0   1  360   WPA2 CCMP   PSK  wifi
A8:42:A1:3F:6D:52   -1        0        0    0   1   -1                   <length:  0>
1E:EC:DA:0F:96:6A  -72       11       93   18  11  130   WPA2 CCMP   PSK  DOSEN_STT
6E:D7:1F:29:F1:F9  -75       36       38    0  11   65   WPA2 CCMP   PSK  queen02
E2:FB:D7:06:A2:D3  -45       43        3    0  12   54   WPA3 CCMP   SAE  realme C53
8E:0B:B2:F0:F2:A0  -53       42        0    0  11   65   WPA2 CCMP   PSK  Martiningsih
BA:EA:04:E8:78:D7  -64       48        1    0  11  360   WPA2 CCMP   PSK  S20
6A:B4:1C:7F:A5:11  -61       28        2    0   6  180   WPA2 CCMP   PSK  Aku siapa?
A8:7D:12:B2:2A:D6  -50       43        5    0   8  130   WPA2 CCMP   PSK  HUAWEI-2AD6
0E:36:0A:56:49:F5  -73       15        2    0   6  180   WPA2 CCMP   PSK  Redmi Note 10S
26:3E:95:58:56:B4  -55       46        0    0   6  360   WPA2 CCMP   PSK  POCO F3
3E:70:9D:60:9A:E0  -50       44       34    1   6  180   WPA2 CCMP   PSK  Rav1
8A:D6:93:2C:B3:9B  -73        3        0    0   5  180   WPA2 CCMP   PSK  real

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

62:67:A5:DE:E7:09  E4:60:17:2C:B5:19  -61    0 - 6e     0         2
FE:EC:DA:0F:96:6A  EA:98:9B:47:88:57  -38    0 - 1    443        99         AUDITORIUM 1
5E:26:36:90:6A:A4  D0:39:57:A6:BB:13   -1    1e- 0      0         1
B0:4E:26:B9:6B:B6  BC:F1:71:49:9B:34  -76    1e- 1     32        16         LAB_IOT
78:45:58:3A:6E:42  8E:AA:58:D4:3F:81  -70    2e- 6     16       195
```

Gambar 9 *Scanning* Aircrack-ng

Hasil pemindaian jaringan menggunakan aircrack-ng dengan perintah airodump-ng akan menampilkan daftar jaringan nirkabel yang terdeteksi di sekitar. Informasi yang ditampilkan mencakup BSSID (alamat MAC dari akses poin), PWR (kekuatan sinyal), Beacons (jumlah sinyal beacon yang dikirimkan oleh akses poin), #Data (jumlah paket data yang diterima), #/s (jumlah paket per detik), CH (channel yang digunakan), MB (kecepatan data maksimum), ENC (jenis enkripsi), CIPHER (algoritma enkripsi yang digunakan), AUTH (metode otentikasi), dan ESSID (nama jaringan).

Scanning Wifite

Selain *scanning* menggunakan aircrack-ng dilakukan juga *scanning* wifite Sehingga informasi mengenai jaringan yang akan menjadi target pengujian serangan *Evil Twin* akan lebih mudah diidentifikasi ke tahap selanjutnya.

(2024), 2 (11): 193-214 Scientica 3021-8209
Jurnal Ilmiah Sain dan Teknologi

Gambar 10 *Scanning* wifite

Sementara itu, hasil pemindaian menggunakan Wifite mencakup NUM (nomor urut jaringan), ESSID (nama jaringan), CH (channel yang digunakan), ENCR (jenis enkripsi), PWR (kekuatan sinyal), dan CLIENT (jumlah klien yang terhubung).
Data ini sangat berguna untuk mengidentifikasi target yang berpotensi menjadi sasaran pengujian serangan Evil Twin, memungkinkan peneliti untuk memilih jaringan dengan kelemahan keamanan yang dapat dieksploitasi dan aktivitas klien yang terhubung.

Threat Modelling (Pemodelan Ancaman)

Pada tahap *threat modelling* (pemodelan ancaman) hasil *scanning* jaringan nirkabel mulai diidentifikasi. *Scanning* tersebut dapat menjadi informasi yang berguna untuk menentukan target yang sesuai.

Identifikasi Ancaman

Dari hasil scanning, didapat informasi dan identifikasi ancaman. Kelemahan-kelemahan yang berpotensi menjadi target penyerangan diidentifikasi sebagai berikut:

Tabel 1 Identifikasi Ancaman

No	Identifikasi Ancaman	Ancaman Terkait
1	Adanya jaringan tanpa enkripsi (OPN) yang memungkinkan akses bebas	Potensi pencurian data karena kurangnya perlindungan enkripsi
2	Menggunakan enkripsi WPA yang lebih lemah dibandingkan WPA2 atau WPA3	Rentan terhadap serangan karena enkripsi yang tidak kuat
3	Penggunaan SSID default yang memudahkan identifikasi jaringan dan target serangan	Penyerang mudah mengidentifikasi dan menyerang jaringan
4	Jaringan dengan nama SSID yang mudah ditebak atau menarik perhatian	Meningkatkan risiko serangan karena penyerang tertarik
5	Banyaknya jaringan dengan kekuatan sinyal rendah	Potensi interferensi atau area rentan
6	Tidak menggunakan SSID tersembunyi untuk jaringan sensitif	Mudah diidentifikasi oleh penyerang
7	Jaringan dengan banyak pengguna yang bisa menjadi target serangan DoS	Rentan terhadap serangan DoS
8	Tidak ada pembatasan akses berdasarkan perangkat tertentu (MAC filtering tidak diaktifkan)	Rentan terhadap spoofing alamat MAC
9	Menggunakan kata sandi yang lemah atau default untuk WPA2-PSK	Rentan terhadap serangan brute force
10	Banyaknya jaringan yang dapat ditemukan dalam waktu singkat	Meningkatkan risiko interferensi dan serangan
11	Penggunaan jaringan nirkabel tanpa otentikasi yang kuat (misalnya hanya berdasarkan SSID)	Rentan terhadap serangan Evil Twin di mana penyerang meniru SSID yang sama

Tabel di atas merinci berbagai kelemahan yang ditemukan dari hasil scanning, memberikan identifikasi setiap ancaman dan menjelaskan ancaman terkait, termasuk ancaman yang berkaitan dengan serangan Evil Twin. Ancaman nomor 11 secara khusus menyoroti risiko serangan Evil Twin, di mana penyerang dapat meniru SSID yang sama untuk menarik pengguna dan mencuri data mereka.

Penentuan Target Pengujian

Tabel 2 Target Jaringan

No	Nama Jaringan	Jenis Enkripsi	CIPHER	Metode Otentikasi
1	LAB_IOT	WPA2	CCMP	PSK
2	AUDITORIUM 1	WPA2	CCMP	PSK

Target yang dipilih untuk pengujian adalah jaringan LAB_IOT dan AUDITORIUM 1. Pemilihan ini didasarkan pada hasil identifikasi ancaman yang menunjukkan bahwa kedua jaringan tersebut memiliki potensi kerentanan yang signifikan. Jaringan LAB_IOT dan AUDITORIUM 1 memiliki karakteristik yang membuatnya menarik untuk pengujian, seperti tingkat enkripsi, kekuatan sinyal, dan aktivitas jaringan yang terdeteksi selama proses pemindaian.

Vulnerability Analysis (*Analisis Kerentanan*)

Hasil dari penentuan target pada tahap ini adalah mencari celah keamanan atau kerentanan pada jaringan LAB_IOT dan AUDITORIUM 1. Celah-celah ini dapat dieksploitasi oleh penyerang untuk melancarkan serangan, termasuk:

Tabel 3 Analisis kerentanan

No	Celah Keamanan	Dampak Potensial
1	PSK (Pre-Shared Key) yang mudah ditebak atau lemah	Penyerang dapat membuat jaringan palsu dengan PSK serupa.
2	Ketidakamanan pada protokol WPA2	Celah keamanan jika perangkat tidak diperbarui.
3	Kurangnya otentikasi saluran (channel authentication)	Penyerang dapat meniru jaringan dengan nama SSID yang sama.
4	Ketidakmampuan perangkat untuk memverifikasi otentikasi jaringan	Rentan terhadap serangan Evil Twin dengan jaringan palsu.

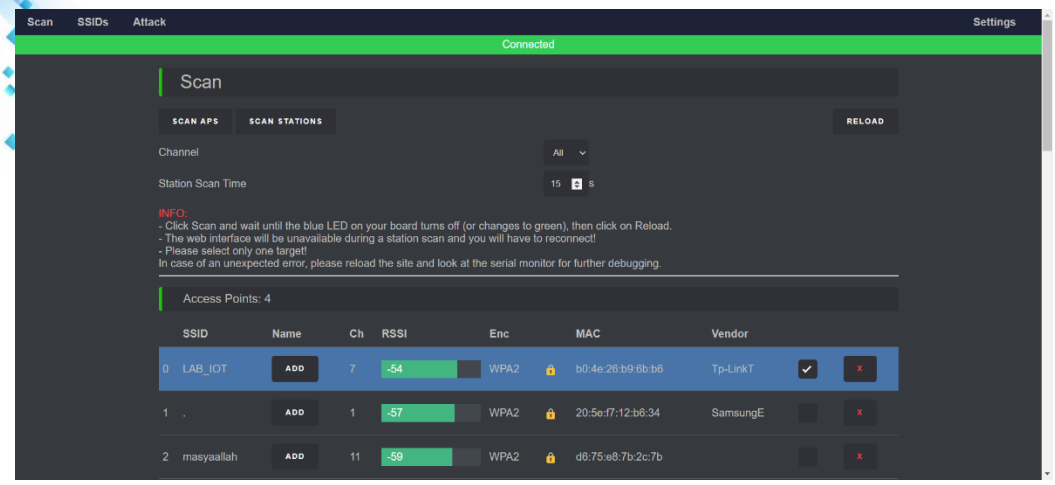
Penilaian ini penting untuk memahami potensi risiko keamanan yang terkait dengan jaringan untuk dilakukan uji simulasi serangan. menguji secara langsung seberapa besar kerentanan yang telah diidentifikasi dapat dieksploitasi oleh penyerang.

Exploitasi (*Uji Simulasi Serangan*)

Pada tahap ini merupakan bagian dari upaya untuk menguji keamanan jaringan secara langsung dengan mensimulasikan serangan yang mungkin dilakukan oleh penyerang pada target LAB_IOT dan AUDITORIUM 1.

***Deauthentification Wi-fi* LAB_IOT**

Proses pertama yaitu mematikan *wi-fi* LAB_IOT sehingga pengguna tidak dapat mengakses jaringan LAB_IOT. Hal ini berguna untuk memaksa pengguna mengakses AP palsu yang dibuat oleh peneliti. Proses *deauthentification* dilakukan dengan ESP8266 *deauthentification* seperi gambar 11 dibawah ini.

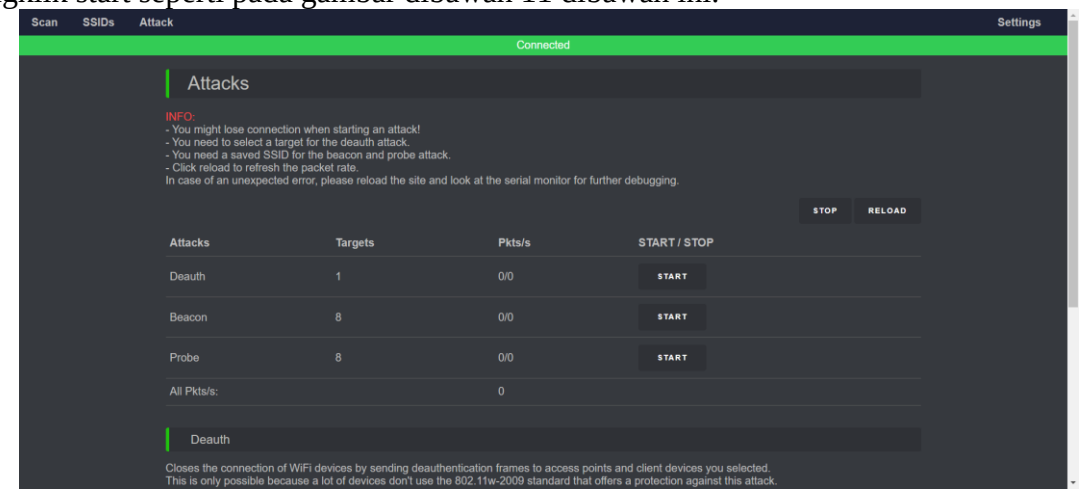


Gambar 10 Proses *deauthentification* LAB_IOT

Menartegkan LAB_IOT sebagai jaringan yang akan *deauthentification* dengan masuk ke *interface deauthentification.* Nyalakan ESP8266 *deauthentification* kemudian hubungkan selanjutnya masuk ke chrome dan masukan 192.168.4.1 maka akan langsung masuk ke *interface deauthentification*. ceklis LAB_IOT dan lakukan attack.

***Attack Deauthentification* LAB_IOT**

Setelah menceklis LAB_IOT masuk ke attack mulai lakukan *deauthentification* dengan mengklik start seperti pada gambar dibawah 11 dibawah ini.

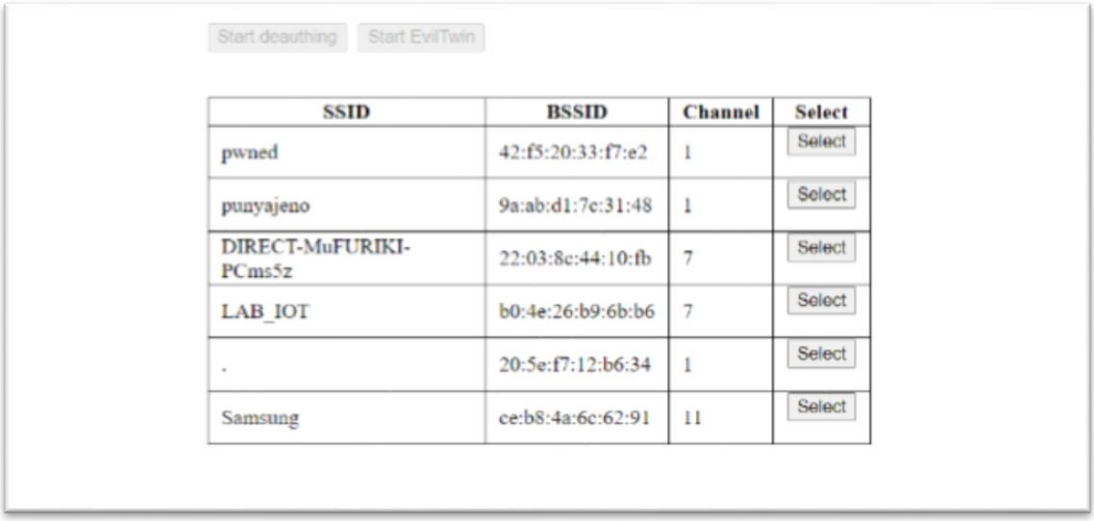


Gambar 11 *attack deauthentification* LAB_IOT

Proses deauthentification yang sedang berlangsung menyebabkan LAB_IOT tidak akan bisa diakses oleh pengguna. Dalam kondisi ini, jika pengguna tetap berusaha untuk terhubung ke jaringan LAB_IOT asli, mereka akan terus-menerus mengalami pemutusan koneksi dan terpental dari jaringan tersebut. Ini terjadi karena penyerang menggunakan teknik deauthentification untuk mengganggu koneksi antara pengguna dan Access Point asli, memaksa mereka untuk mencari jaringan alternatif. Akibatnya, pengguna yang frustrasi karena tidak bisa mengakses LAB_IOT asli lebih mungkin untuk terjebak oleh AP palsu yang telah dibuat oleh penyerang, sehingga berpotensi memberikan kredensial login mereka tanpa sadar.

Pembuatan *Acces Point* Palsu LAB_IOT

Pembuatan Access Point (AP) palsu LAB_IOT sebagai upaya mendapatkan password dari jaringan LAB_IOT dengan menggunakan perangkat keras ESP8266. Menjebak pengguna yang tidak bisa mengakses LAB_IOT asli agar terkecoh dan masuk ke dalam AP palsu yang telah disiapkan oleh penyerang. Dengan demikian, ketika pengguna mencoba mengakses jaringan LAB_IOT melalui AP palsu untuk mendapatkan password, yang digunakan oleh pengguna untuk masuk ke jaringan tersebut.

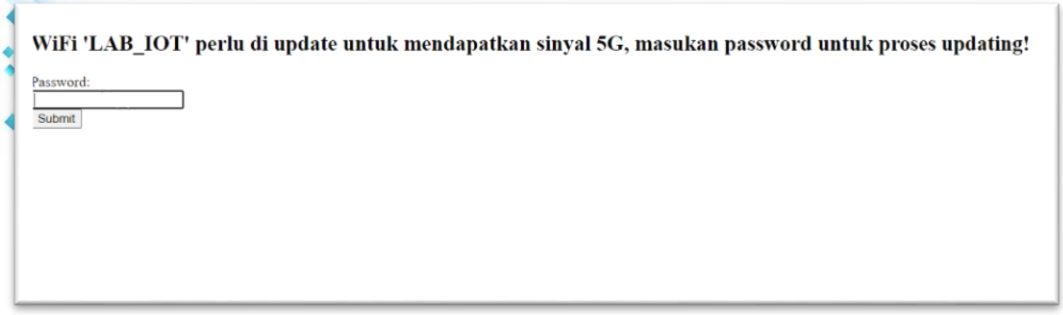


Gambar 12 Pembuatan AP palsu LAB_IOT

Nyalakan perangkat ESP8266 Evil Twin. Setelah perangkat menyala, hubungkan perangkat yang ingin digunakan untuk mengakses jaringan, seperti laptop atau smartphone, ke jaringan Wi-Fi yang disediakan oleh ESP8266 Evil Twin. Setelah berhasil terhubung ke jaringan Wi-Fi ESP8266 Evil Twin, buka peramban web seperti Google Chrome pada perangkat tersebut. Di bilah alamat Chrome, masukkan alamat IP 192.168.4.1 untuk mengakses antarmuka konfigurasi ESP8266 Evil Twin. Setelah antarmuka terbuka, cari dan pilih jaringan LAB_IOT dari daftar jaringan yang tersedia. Setelah memilih LAB_IOT, klik tombol "Start Evil Twin" untuk memulai proses pembuatan Access Point palsu yang akan meniru jaringan LAB_IOT, dengan tujuan menjebak pengguna lain untuk terhubung dan memasukkan kredensial login mereka.

Pishing Page LAB_IOT *Evil Twin*

Dengan menyalakan perangkat ESP8266 Evil Twin, muncul halaman phishing yang dirancang untuk menipu pengguna ketika pengguna mencoba mengakses Access Point (AP) palsu yang telah dibuat. Halaman phishing ini menampilkan formulir yang meminta pengguna untuk memasukkan password pengguna, memberikan ilusi bahwa pengguna sedang melakukan login ke jaringan yang sah seperti gambar 13 dibawah ini.

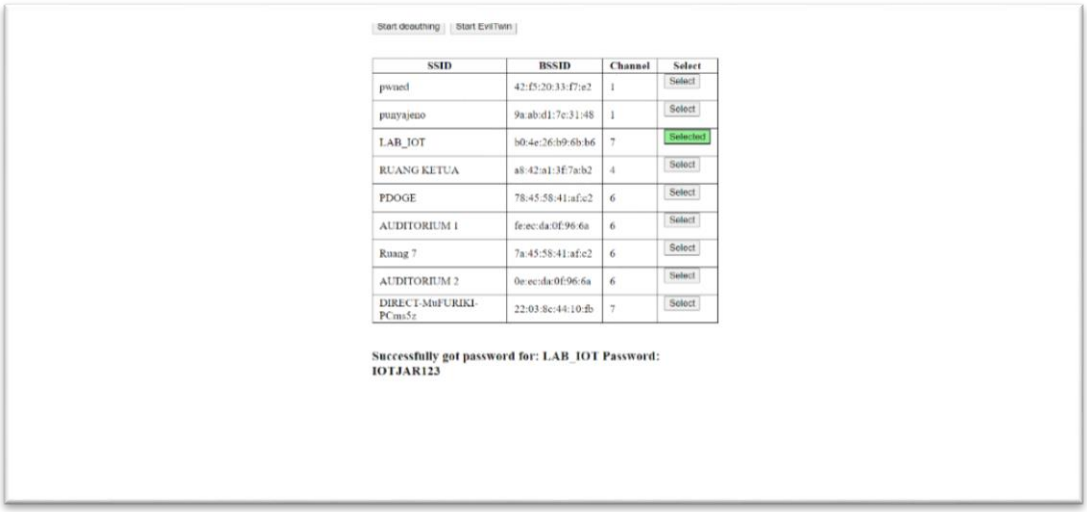


Gambar 13 Pishing page LAB_IOT *Evil Twin*

Ketika pengguna menghubungkan perangkat pengguna ke AP palsu yang meniru jaringan LAB_IOT, pengguna akan secara otomatis diarahkan ke halaman phishing yang tampak sangat mirip dengan halaman login asli dari jaringan LAB_IOT.

Hasil *Password* LAB_IOT

Pada akhir proses, setelah ada pengguna yang memasukkan *password* yang benar ke dalam halaman phishing yang disediakan oleh AP palsu, *password* tersebut akan secara otomatis terekam pada *interface Evil Twin*. Interface ini menampilkan data yang dikumpulkan dari pengguna yang terjebak oleh AP palsu, termasuk *password* yang dimasukan seperti pada gambar 14 dibawah ini.



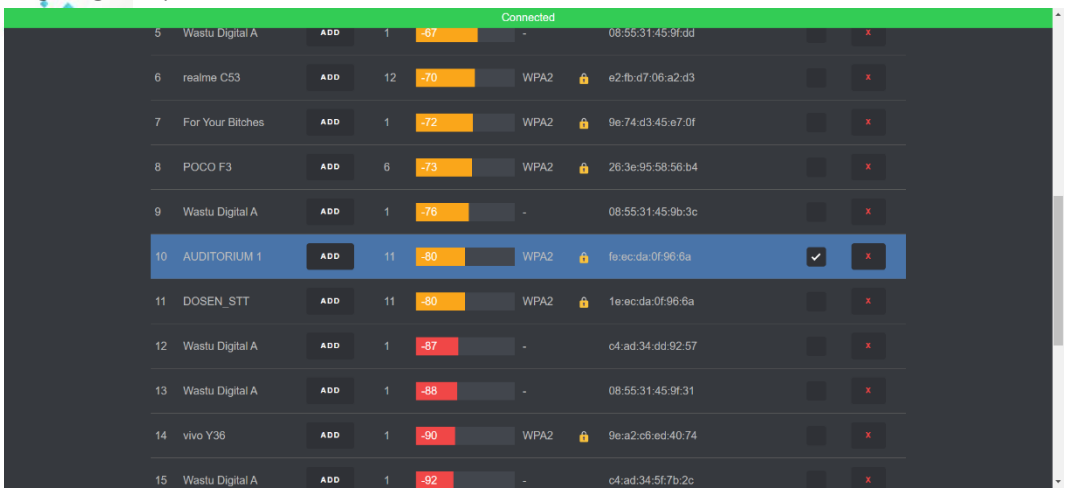
Gambar 14 *Password* LAB_IOT

Didapat Password dari jaringan LAB_IOT yang berhasil didapatkan adalah "IOTJAR123", yang terekam dari pengguna yang terjebak memasukkan password valid pada halaman phishing Evil Twin. Keberhasilan ini menunjukkan bahwa penyerang telah sukses menjalankan serangan Evil Twin, di mana pengguna yang tidak waspada telah ditipu untuk mengungkapkan informasi login mereka. Dengan berhasil memperoleh password ini, proses pengujian serangan Evil Twin terhadap jaringan nirkabel LAB_IOT dapat dianggap berhasil.

***Deauthentification Wi-fi* AUDITORIUM 1**

Setelah berhasil melancarkan serangan terhadap jaringan LAB_IOT, langkah berikutnya adalah mematikan Wi-Fi AUDITORIUM 1 untuk mencegah pengguna mengakses jaringan tersebut. Tindakan ini penting agar pengguna terdorong untuk menggunakan Access Point (AP) palsu yang telah dipersiapkan oleh peneliti. Proses deauthentification akan

dilakukan dengan menggunakan perangkat ESP8266, serupa dengan yang diperlihatkan dalam gambar 11 untuk LAB_IOT, seperti yang terlihat pada gambar 12 di bawah ini untuk AUDITORIUM 1.

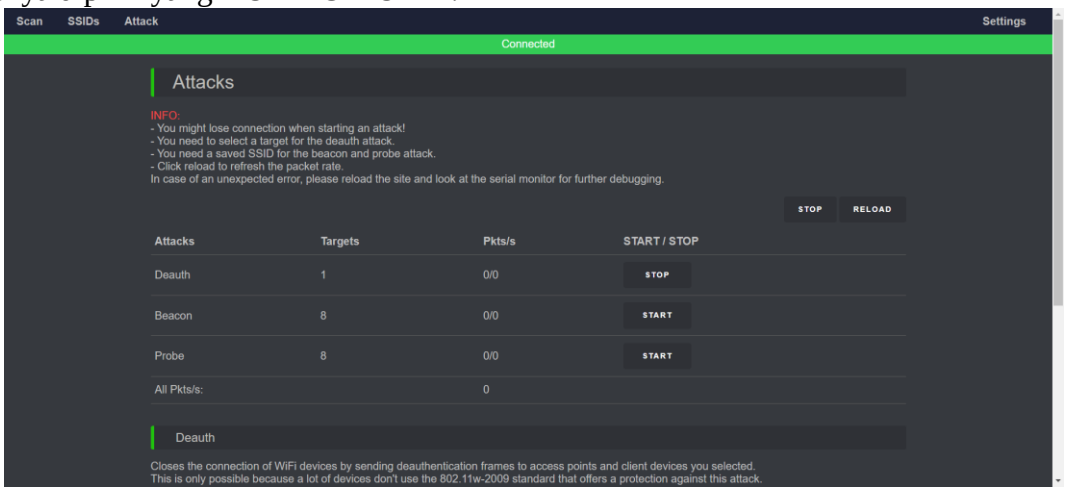


Gambar 12 Proses *deauthentification* AUDITORIUM 1

Untuk melakukan serangan pada AUDITORIUM 1 menggunakan perangkat ESP8266, langkah pertama adalah mengaktifkan perangkat dan menjalankan serangan deauthentification terhadap jaringan tersebut. Setelah itu, perlu membuka peramban web seperti Chrome dan mengakses alamat IP 192.168.4.1. Hal ini akan mengarahkan langsung ke *interface deauthentification*. Di sana, pilih opsi untuk AUDITORIUM 1 dan lanjutkan dengan melaksanakan serangan yang diperlukan.

Attack Deauthentification AUDITORIUM 1

Proses selanjut sama dengan *attack deauthentification* pada LAB_IOT namun disani targtenya dipilih yang AUDITORIUM 1.

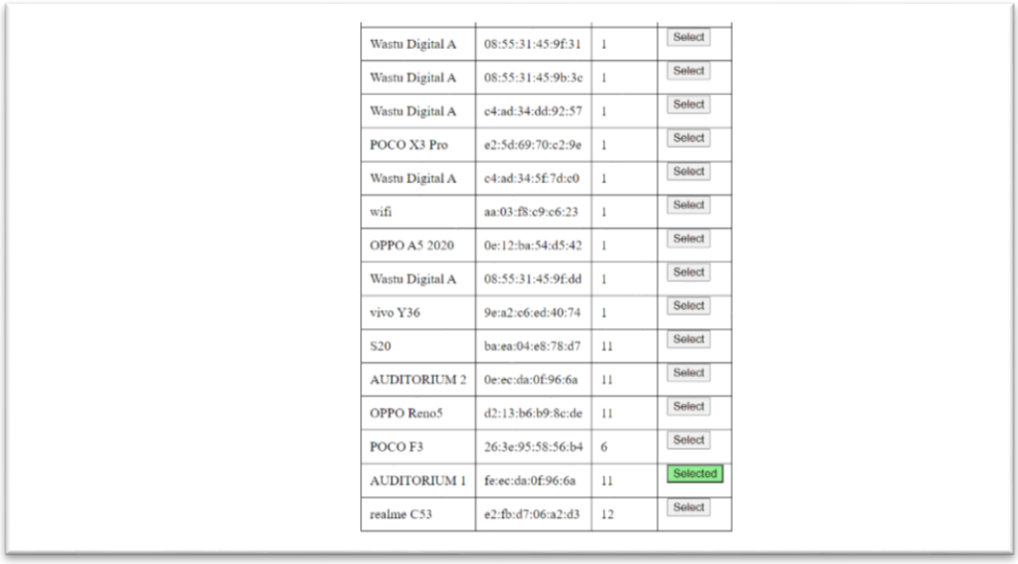


Gambar 13 *attack deauthentification* AUDITORIUM 1

Melakukan *start Deauth* untuk mematikan AUDITORIUM 1 sehingga pengguna tidak bisa mengakses jaringan tersebut memudahkan ke proses pembuatan AP palsu AUDITORIUM 1 pada *Evil Twin*.

Pembuatan *Acces Point* Palsu AUDITORIUM 1

Proses pembuatan AP palsu untuk AUDITORIUM dapat segera dilaksanakan setelah melakukan *deauthentification*, yang dapat signifikan meningkatkan keberhasilan serangan Evil Twin. Dengan menonaktifkan akses pengguna ke jaringan AUDITORIUM 1, langkah berikutnya adalah mengkonfigurasi AP palsu dengan setting yang meniru sinyal dan identitas AUDITORIUM 1.



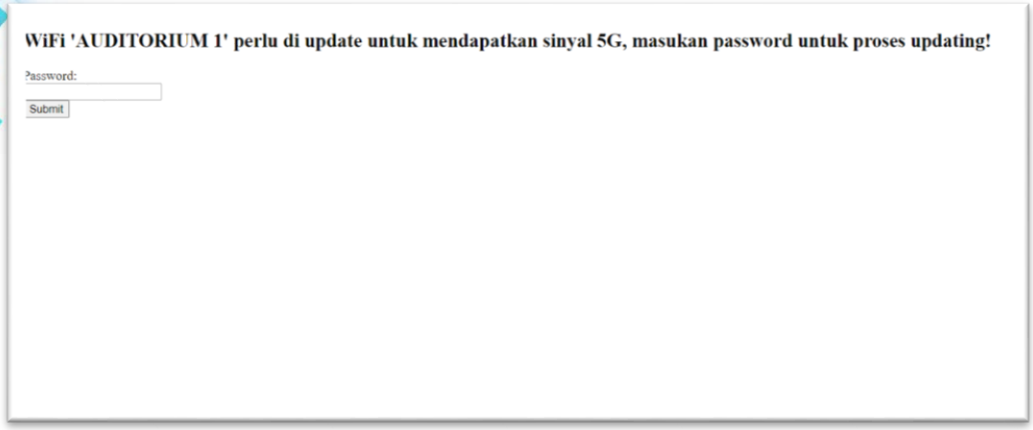
Wastu Digital A	08:55:31:45:9f:31	1	Select
Wastu Digital A	08:55:31:45:9b:3e	1	Select
Wastu Digital A	c4:ad:34:dd:92:57	1	Select
POCO X3 Pro	e2:5d:69:70:c2:9e	1	Select
Wastu Digital A	c4:ad:34:5f:7d:c0	1	Select
wifi	aa:03:f8:c9:c6:23	1	Select
OPPO A5 2020	0e:12:ba:54:d5:42	1	Select
Wastu Digital A	08:55:31:45:9f:dd	1	Select
vivo Y36	9e:a2:c6:ed:40:74	1	Select
S20	ba:ea:04:e8:78:d7	11	Select
AUDITORIUM 2	0e:ec:da:0f:96:6a	11	Select
OPPO Reno5	d2:13:b6:b9:8c:de	11	Select
POCO F3	26:3e:95:58:56:b4	6	Select
AUDITORIUM 1	fe:ec:da:0f:96:6a	11	Selected
realme C53	e2:fb:d7:06:a2:d3	12	Select

Gambar 14 Pembuatan AP palsu AUDITORIUM 1

Setelah berhasil menjalankan serangan LAB_IOT, langkah selanjutnya adalah melakukan serangan terhadap AUDITORIUM 1. Untuk melanjutkan proses ini, perlu mengonfigurasi ulang perangkat ESP8266 Evil Twin. Pastikan perangkat telah terhubung kembali ke antarmuka konfigurasi dengan memasukkan alamat IP 192.168.4.1 ke dalam Google Chrome pada perangkat yang terhubung. Setelah masuk ke *interface* konfigurasi, cari dan pilih jaringan AUDITORIUM 1 dari daftar jaringan yang tersedia. Selanjutnya, klik tombol "Start Evil Twin" untuk memulai proses pembuatan *Access Point* palsu yang meniru jaringan AUDITORIUM 1, dengan tujuan menarik pengguna lain untuk terhubung dan mengungkapkan kredensial login mereka.

Pishing Page AUDITORIUM 1 *Evil Twin*

Pada tahap ini, setelah berhasil menyiapkan serangan Evil Twin terhadap jaringan AUDITORIUM 1, langkah selanjutnya adalah membuat halaman phishing (pishing page) yang akan digunakan untuk menipu pengguna yang terhubung ke access point palsu tersebut. Halaman phishing ini dirancang sedemikian rupa agar terlihat seperti halaman masuk resmi atau halaman informasi yang sah dari jaringan AUDITORIUM 1 seperti pada gambar.

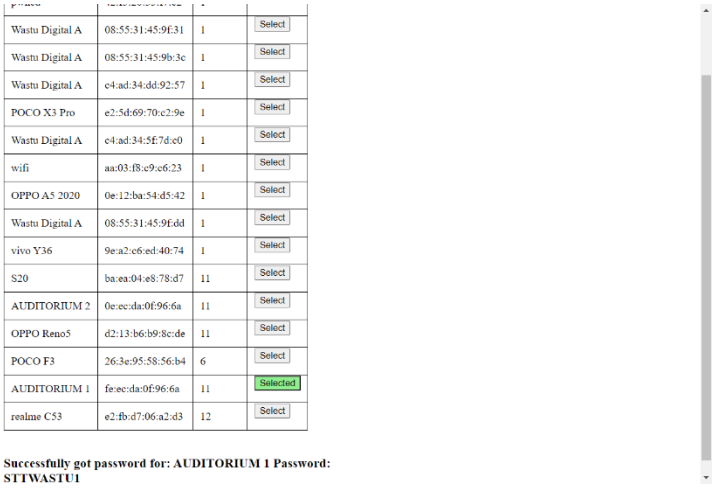


Gambar 15 Pishing page AUDITORIUM 1 *Evil Twin*

Pengguna yang memasukkan password AUDITORIUM 1 yang benar secara tidak sadar akan membuat password tersebut terekam oleh penyerang. Dengan kata lain, informasi login yang sensitif ini akan tercatat dan dapat digunakan oleh penyerang untuk mengakses jaringan AUDITORIUM 1. Hal ini memungkinkan penyerang untuk masuk ke jaringan tersebut.

Hasil *Password* AUDITORIUM 1

Pengguna yang telah memasukan password AUDITORIUM 1 yang benar hasil password tersebut dan akan terekam muncul di interface Evil Twin dibagian paling bawah seperti pada gambar 16



Gambar 16 *Password* AUDITORIUM 1

Jika sudah muncul "successfully got password for AUDITORIUM 1" maka serangan telah berhasil. Bisa dilihat password dari AUDITORIUM 1 adalah "STTWASTU1".

Reporting

Dalam tahap *Reporting* ini, hasil uji coba terhadap keamanan jaringan LAB_IOT dan AUDITORIUM 1 telah berhasil didokumentasikan. Melalui pengujian serangan menggunakan Evil Twin dengan perangkat ESP8266, berhasil menunjukkan rentannya kedua jaringan terhadap serangan yang dapat mengecoh pengguna untuk terhubung ke Access Point (AP) palsu. Langkah-langkah seperti deauthentification berhasil mematikan koneksi Wi-Fi pada

kedua jaringan, memaksa pengguna untuk mencari jaringan alternatif yang merupakan AP palsu.

Hasil Pengujian

Dari pengujian serangan Evil Twin, peneliti berhasil memperoleh hasil dari pengujian yang dilakukan pada dua jaringan, yaitu LAB_IOT dan AUDITORIUM 1. Hasil pengujian ini dapat dilihat pada tabel 4 di bawah ini.

Tabel 4 Hasil Pengujian

Nama Jaringan	Jenis Enkripsi	Hasil Serangan	Status
LAB_IOT	WPA2	*Deauthentification* berhasil dilakukan, pengguna terjebak pada AP palsu, berhasil mendapatkan password "**IOTJAR123**".	BERHASIL
AUDITORIUM 1	WPA2	*Deauthentification* berhasil dilakukan, pengguna terjebak pada AP palsu, berhasil mendapatkan password "**STTWASTU1**".	BERHASIL

Tabel di atas menggambarkan hasil pengujian serangan Evil Twin pada dua jaringan berbeda: LAB_IOT dan AUDITORIUM 1. Kedua jaringan ini menggunakan enkripsi WPA2, yang merupakan standar keamanan Wi-Fi yang banyak digunakan. Meskipun enkripsi WPA2 cukup kuat, serangan Evil Twin dapat memanfaatkan kelemahan dalam proses autentikasi jaringan. Serangan ini dimulai dengan melakukan deauthentification, di mana penyerang memutus koneksi antara pengguna dan Access Point asli, memaksa pengguna untuk mencari jaringan alternatif. Pada jaringan LAB_IOT, serangan deauthentification berhasil memutus koneksi pengguna dari jaringan asli. Pengguna yang terputus kemudian mencari jaringan lain dan tanpa sadar terhubung ke Access Point palsu yang dibuat oleh peneliti. Dalam kondisi ini, peneliti menyediakan halaman phishing yang menyerupai halaman login asli. Ketika pengguna memasukkan password mereka ke dalam halaman phishing ini, peneliti berhasil mendapatkan password tersebut. Hasilnya, password "IOTJAR123" dari jaringan LAB_IOT berhasil diperoleh.

Serangan serupa juga diterapkan pada jaringan AUDITORIUM 1 dengan hasil yang serupa. Pengguna jaringan AUDITORIUM 1 mengalami deauthentification, yang memaksa mereka terputus dari jaringan asli. Mereka kemudian tanpa sadar terhubung ke Access Point palsu yang dikendalikan oleh peneliti. Melalui halaman phishing yang menyerupai halaman login asli, peneliti berhasil mengecoh pengguna untuk memasukkan password mereka. Akhirnya, password "STTWASTU1" dari jaringan AUDITORIUM 1 berhasil diperoleh. Keberhasilan kedua serangan ini menegaskan bahwa meskipun jaringan menggunakan enkripsi WPA2 yang kuat, mereka tetap rentan terhadap serangan yang menargetkan kelemahan dalam proses autentikasi pengguna. Serangan Evil Twin menunjukkan bahwa melalui manipulasi dan rekayasa sosial, penyerang dapat mengecoh pengguna untuk memberikan informasi login yang sensitif.

Data Log Pengujian

Data log pengujian adalah dokumen rinci yang mencatat semua aktivitas dan hasil yang diperoleh selama pengujian serangan Evil Twin pada jaringan LAB_IOT dan AUDITORIUM 1. Dokumen ini mencakup informasi tentang perangkat yang digunakan, langkah-langkah yang diambil selama serangan, dan hasil yang dicapai pada setiap tahap pengujian. Tujuan utama dari data log ini adalah untuk membantu peneliti memahami efektivitas serangan, mengidentifikasi kelemahan dalam jaringan, dan memvalidasi hasil yang diperoleh.

Pada pengujian terhadap jaringan LAB_IOT, data log mencatat proses deauthentification yang berhasil dilakukan, pembuatan Access Point palsu, dan penangkapan password pengguna, yang menunjukkan keberhasilan serangan dengan mendapatkan password "IOTJAR123". Serangan pada jaringan AUDITORIUM 1 juga didokumentasikan dengan detail dalam data log, mencatat proses deauthentification, pembuatan Access Point palsu, dan penggunaan halaman phishing untuk menangkap password pengguna, yang berhasil mendapatkan password "STTWASTU1". Data log ini memberikan informasi yang penting untuk menganalisis efektivitas serangan secara keseluruhan dan membantu pengembangan strategi keamanan yang lebih baik untuk menghadapi serangan-serangan di masa depan. Tabel log serangan dapat dilihat pada tabel 5.

Tabel 5 Data Log Pengujian

Pengujian	Target pengujian	Waktu Pengujian	Hasil Pengujian
Pengujian 1	LAB_IOT	8 Mei 2024	Berhasil *deauthentification* Gagal mendapat password
Pengujian 2	LAB_IOT	15 Mei 2024	Berhasil *deauthentification* Gagal mendapat password
Pengujian 3	LAB_IOT	20 Mei 2024	Berhasil *deauthentification* Gagal mendapat password
Pengujian 4	LAB_IOT	22 Mei 2024	Berhasil deauthentification Berhasil mendapat password LAB_IOT “IOTJAR123”
Pengujian 5	AUDITORIUM 1	27 Mei 2024	Berhasil *deauthentification*

Pengujian	Target pengujian	Waktu Pengujian	Hasil Pengujian
			Gagal mendapat password
Pengujian 6	AUDITORIUM 1	3 Juni 2024	Berhasil *deauthentification*
			Gagal mendapat password
Pengujian 7	AUDITORIUM 1	10 Juni 2024	Berhasil *deauthentification*
			Gagal mendapat password
			Berhasil deauthentification
Pengujian 8	AUDITORIUM 1	12 Juni 2024	Berhasil mendapat password AUDITORIUM 1 "STTWASTU1"

Data log yang tercatat mencerminkan hasil dari serangkaian uji coba terhadap serangan Evil Twin pada jaringan LAB_IOT dan AUDITORIUM 1. Setiap entri dalam data log ini mencatat apakah serangan deauthentification berhasil dilakukan dan apakah peneliti berhasil memperoleh password dari jaringan yang diserang. Pada jaringan LAB_IOT, terdapat empat pengujian yang tercatat, di mana pada tiga pengujian pertama, deauthentification berhasil namun upaya untuk mendapatkan password tidak berhasil. Hanya pada uji coba keempat, deauthentification berhasil dilakukan dan peneliti berhasil memperoleh password "IOTJAR123" dari jaringan LAB_IOT.

Sama halnya dengan jaringan LAB_IOT, pengujian pada jaringan AUDITORIUM 1 juga mencatat empat percobaan serangan. Meskipun deauthentification berhasil dalam keempat pengujian tersebut, upaya untuk mendapatkan password hanya berhasil pada uji coba terakhir. Peneliti berhasil memperoleh password "STTWASTU1" dari jaringan AUDITORIUM 1, sedangkan dalam tiga pengujian sebelumnya, usaha untuk mendapatkan password tidak berhasil.

Data log ini menggambarkan bahwa meskipun serangan deauthentification berhasil dilakukan dalam sebagian besar pengujian, keberhasilan dalam memperoleh password dari jaringan yang diserang bervariasi. Faktor-faktor seperti respons pengguna terhadap serangan dan kemungkinan kegagalan teknis juga mempengaruhi hasil dari serangan Evil Twin.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan penelitian yang telah dilakukan, serangan *Evil Twin* pada jaringan nirkabel terbukti sebagai ancaman serius yang dapat mengeksploitasi kelemahan keamanan, terutama pada jaringan dengan protokol keamanan lemah atau kata sandi default. Penelitian ini

menggunakan ESP8266 dan metode *Penetration Testing* untuk mensimulasikan serangan, yang menunjukkan bahwa serangan Evil Twin dapat dilakukan dengan efektif. Penelitian dilaksanakan di lingkungan jaringan Sekolah Tinggi Teknologi Wastukancana (STT Wastukancana), yang memiliki infrastruktur jaringan kompleks dengan beragam pengguna seperti mahasiswa, dosen, dan staf administrasi. Hasil penelitian menegaskan perlunya peningkatan keamanan jaringan nirkabel melalui penerapan enkripsi yang kuat, deteksi jaringan yang efektif, dan kebijakan pembaruan perangkat lunak secara rutin. Selain itu, penelitian ini memberikan kontribusi pada pemahaman yang lebih baik tentang metode pengujian keamanan jaringan serta memberikan panduan praktis bagi pengguna jaringan dan peneliti dalam memilih langkah-langkah keamanan yang lebih efektif.

Saran

Berdasarkan kesimpulan mengevaluasi peneliti memberikan sejumlah rekomendasi kepada pihak terkait serta untuk penelitian lanjutan.

1. Untuk melakukan penelitian yang memfokuskan pada pengujian keamanan jaringan, khususnya penelitian mengenai serangan *Evil Twin*, disarankan untuk menggunakan perangkat yang lebih kompleks, seperti perbaikan pada halaman phishing untuk *Evil Twin* yang sulit dideteksi.
2. Dalam penelitian selanjutnya, disarankan untuk mengusulkan proses mitigasi dengan menggunakan teknik tertentu untuk mengatasi serangan *Evil Twin*, seperti penggunaan counter yang dapat mencegah serangan tersebut.
3. Untuk melindungi dari serangan Evil Twin, gunakan teknologi keamanan seperti WPA2-Enterprise atau WPA3 untuk enkripsi data dan autentikasi kuat seperti EAP-TLS. Pantau jaringan *Wi-Fi* secara aktif, edukasi pengguna tentang serangan tersebut.
4. Jika menggunakan Kali Linux sebagai alat penelitian, disarankan untuk menghindari penggunaan virtual machine seperti VirtualBox. Jika ingin tetap mempertahankan sistem operasi Windows tanpa menghapusnya, sebaiknya gunakan opsi dual boot.

DAFTAR PUSTAKA

Antoni. (2020). *ANALISIS DAN PENGUJIAN KEMANAN KELEMAHAN JARINGAN NIRKABEL DENGAN METODE EVIL TWIN ATTACK PADA KALI LINUX*. https://doi.org/https://doi.org/10.31219/osf.io/wuqe2

Creswell, J. W. (2019). *Research design pendekatan kualitatif, kuantitatif, dan mixed*.

Dayan, R., Muhyidin, Y., & Singasatia, D. (2023). ANALISIS KEAMANAN JARINGAN PADA WIRELESS LOCAL AREA NETWORK TERHADAP SERANGAN BRUTE FORCE MENGGUNAKAN METODE PENETRATION TESTING. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *7*, 2051–2056. https://doi.org/10.36040/jati.v7i3.7097

Dewi, N. H. L., Rohmah, M. F., & Zahara, S. (2020). *PROTOTYPE SMART HOME DENGAN MODUL NODEMCU ESP8266 BERBASIS INTERNET OF THINGS (IOT)*.

Hayaty, N., & Cs, M. (2020). *Buku Ajar: Sistem Keamanan*.

Maslan, A., & & Wangdra, T. (2019). *Belajar Cepat Teori, Praktek dan Simulasi Jaringan Komputer & Internet*.

Mei Lina, I., & Ryan Fernandes, G. (2022). ANALISIS POLA SOSIAL ENGINEERING MENGGUNAKAN TEKNIK WIFI DEAUTHER DAN EVIL TWIN. *Jurnal Rekayasa Komputasi Terapan)*, *02*, 2776–5873.

Mulyanto, Y., Herfandi, H., & Candra Kirana, R. (2022). ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING (Studi kasus:RS H.LMANAMBAI ABDULKADIR). *Jurnal Informatika Teknologi Dan Sains*, *4*(1), 26–35. https://doi.org/10.51401/jinteks.v4i1.1528

Mulyanto, Y., Herfandi, & Kirana, R. C. (2022). *ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING (Studi kasus:RS H.LMANAMBAI ABDULKADIR)*.

Mustafa, H., & Xu, W. (2019). *Detecting evil twin access point attacks in wireless hotspots. In 2019 IEEE Conference on Communications and Network Security*. https://doi.org/https://doi.org/10.1109/CNS.2014.699 7491

Nakhila, & Zou. (2019). *User-side Wi-Fi evil twin attack detection using random wireless channel monitoring*.

NANIK, S. (2021). *Jaringan Dasar* . 157.

Nikbakhsh, S., Manaf, A. B. A., Zamani, M., & Janbeglou, M. (2019). *A novel approach for rogue access point detection on the client-side. In Proceedings - 26th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2019*. 684–687. https://doi.org/https://doi.org/10.1109/WAINA.2012.

Onno W, P. (2020). *Buku Pegangan Internet Wireless dan Hot Spot*.

Panch, A., & Singh, S. K. (2020). *A novel approach for evil twin or rogue AP mitigation in wireless environment. International Journal of Security and its Applications*.

Peniarsih. (2021). *PENERAPAN EVIL TWIN DETEKTOR DALAM PENDETEKSIAN PENGGANGGU JARINGAN NIRKABEL PADA USER*.

Priyambodo, T. K. (2020). *Jaringan Wi-Fi, Teori dan Implementasi*.

Rachman, R. (2021). *ANALISIS KEAMANAN JARINGAN WIRELESS LAN (WLAN) DENGAN METODE PENETRATION TESTING PADA PT.PLN (PERSERO) SEKTOR PENGENDALIAN PEMBANGKITAN PEKANBARU*.

Rinaldi, R., & Sadikin, M. (2019). *Analisa dan Pengujian Serangan Evil Twin pada Jaringan berbasis Wireless dengan Keamanan WPA2-PSK Mujiono Sadikin*. https://www.researchgate.net/publication/335929306

Rusdi, M. I., & Prasti, D. (2019). Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux. *Seminar Nasional Teknologi Informasi Dan Komputer*.

Satria Galang Saputra, Parga Zen, B., & Abdurahman. (2023). Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing Execution Standard (PTES). *Jurnal Sistem Informasi Galuh*, *1*(2), 43–51. https://doi.org/10.25157/jsig.v1i2.3152

Schepers, D., Ranganathan, A., & Vanhoef, M. (2022). On the Robustness of Wi-Fi Deauthentication Countermeasures. *WiSec 2022 - Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 245–256. https://doi.org/10.1145/3507657.3528548

Setyawan, F., & Amnur, H. (2022). *Keamanan Jaringan Wireless Dengan Kali Linux*. *3*(1), 16–22. http://jurnal-itsi.org

Stevi, K., Sumendap, S., & Koagouw, F. V. I. A. (2019). *PENTINGNYA PENGGUNAAN JARINGAN WI-FI DALAM MEMENUHI KEBUTUHAN INFORMASI PEMUSTAKA PADA KANTOR PERPUSTAKAAN DAN KEARSIPAN DAERAH KOTA TIDORE KEPULAUAN*.

Utomo, E. P. (2019). *Wireless Networking*.

Weidman, G. (2022). *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press. https://books.google.co.id/books?id=DUMyDwAAQBAJ