Jurnal Informa : Jurnal Penelitian dan Pengabdian Masyarakat. p-ISSN : 2442-7942, e-ISSN 2716-5051
Volume 8 Nomor 1 Juni 2022

Implementasi Metode *Mac Spoofing* Pada Wifi Jammer NodeMCU ESP8266 Di Client Windows 10

Galah Seno Adjie[1)], Kustanto[2)], Bebas Widada[3)]

[1)] Program Studi Informatika (S-1), STMIK Sinar Nusantara
[2)] Program Studi Teknologi Informasi (D-3), STMIK Sinar Nusantara
[3)] Program Studi Sistem Informasi (S-1), STMIK Sinar Nusantara
Jl. K.H Samanhudi No.84-86, Purwosari, Kec. Laweyan, Surakarta, Jawa Tengah 57149
[1]galahsenoadjie@gmail.com, [2]kustanto@sinus.ac.id, [3]bbswdd@yahoo.com

Abstract

With the development of the increasingly fast especially in the areas of network technology, users are expected to to keep track of it so as not to lose by other users. The need for a new wifi network is becoming a basic requirement for the community both for the students and for the workers, the presence of unexpected events the client disconnected from wifi router which resulted in the absence of a direct internet connection without any warning or commonly called wifi jammer. In the current research aims to create a program for clients to avoid wifi jammer, this program works by changing the client mac address or usually called mac spoofing method which are run by the client, with a new registry file filled into the directory automatic batch file with regedit to get the new mac address. The program uses the Java netbeans GUI to simplify operations by clients, a different configs can be used automatically. The results of this program in the form of a new mac address will be shown in the program can to avoid a wifi jammer.

Keywords: Wifi Jammer, Registry, Batch File, Netbeans

1. PENDAHULUAN

Disconnection wifi client menggunakan ESP8266 dilakukan dengan scan AP (*access point*) yang terkoneksi internet berdasarkan *mac address* client. M*ac address* merupakan hal yang bersifat unik pada setiap *interface* smartphone ataupun laptop.

Mac address (*Media Access Control Address*) merupakan sebuah alamat yang di implementasikan pada lapisan data link dalam tujuh lapisan model *OSI* (*Open System Interconnection*), yang berguna untuk mengidentifikasi seluruh perangkat jaringan secara unik agar dapat terhubung dan berkomunikasi dalam sebuah jaringan. *Mac address* setiap *interface* adalah berbeda dengan setiap *interface* yang lain, bersifat karakter unik panjangnya 6 byte.

Di penelitian ini client yang terserang wifi jammer esp8266 hanya bisa terhindar dengan cara merubah alamat *mac address*nya ke alamat baru sehingga client bisa mendapatkan koneksi ke *access point.* Merubah alamat *mac address* bisa dilakukan secara manual, namun tidak semua client wifi yang terserang wifi jammer bisa dirubah alamat *mac address* nya secara manual.

Untuk mengatasi masalah tersebut dibutuhkan program untuk memudahkan client dalam merubah *mac address*nya secara otomatis.

2. METODE PENELITIAN

a. Analisa sistem

Analisa terhadap sistem yang akan dibuat dilakukan dengan menggunakan diagram alir. Diagram alir atau biasa disebut flowchart merupakan sebuah diagram dengan symbol-symbol grafis yang menyatakan aliran atau proses yang menampilkan langkah-langkah yang disimbolkan dalam bentuk kota, beserta urutanya dengan menghubungkan masing-masing langkah tersebut menggunakan tanda panah. Diagram ini dapat memberi solusi sekaligus dapat digunakan untuk menganalisi selangkah demi selangkah dalam proses penyelesaian masalah yang dihadapi. Diagram yang nantinya akan dibuat sesuai dengan cara kerja sistem yang akan berjalan.

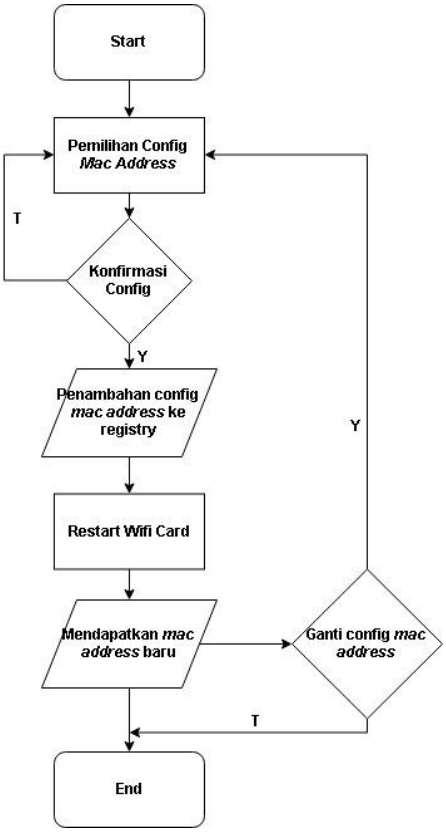
b. Analisa kebutuhan sistem

1) Analisa Kebutuhan Perangkat Keras (Hardware)

Suatu sistem utama dari sebuah sistem computer secara fisik yang terdiri dari komponen-komponen yang saling terkait antara input, proses, dan output.

2) Analisa Kebutuhan Perangkat Lunak (Software)

Sekumpulan perintah-perintah untuk menjalankan perangkat keras. Perangkat lunak yang peneliti gunakan untuk membuat dan mengoperasikan aplikasi adalah NetBeans IDE, Regedit, dan Batch file. Berikut adalah Gambar 1 flowchart:



Gambar 1. Flowchart Program

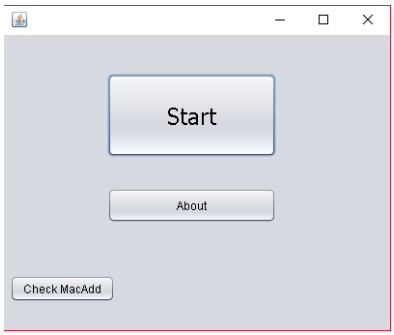
c. Desain Tampilan

Desain tampilan sistem ini dirancang dengan tujuan agar pada saat pembuatan sistem mac spoofing dengan tampilan aplikasi lebih mudah.

Berikut desain tampilan yang memuat program:

1) Tampilan Awal

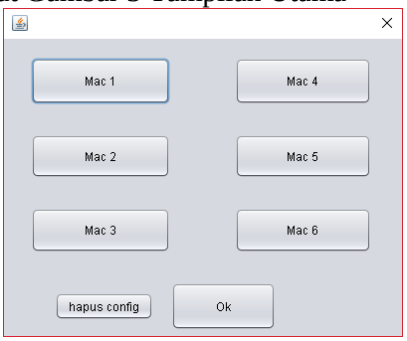
Tampilan awal berisikan tampilan yang disajikan kepada user pada saat program pertama kali di jalankan. Berikut merupakan Gambar 2 tampilan awal



Gambar 2. Tampilan Awal

2) Tampilan Utama Program

Tampilan utama merupakan inti dari program ini, berisikan beberapa tombol config mac address, hapus config, dan tombol save. Berikut Gambar 3 Tampilan Utama



Gambar 3. Tampilan Utama

d. Tahapan Penelitian

Penelitian ini dimulai dari mengidentifikasi masalah, membuat hipotesa, studi pustaka, pembuatan program, pengujian dan perbaikan program, dan terakhir adalah pembuatan desain program, Gambar 4 di bawah menampilkan tahapan penelitian.

Gambar 4. Tahapan Peneliti

3. TINJAUAN PUSTAKA

a. F.Eka (2017) Kontrol dan monitoring smarthome dengan modul esp8266 serta server thinkspeak. Hasil yang didapatkan lampu dapat di nyalakan dan di padamkan melalui web panel yang berjalan di web server pada Modul ESP 8266 dan diakses melalui web browser smartphone, komputer atau laptop melalui jaringan WiFi [1]

b. M. Nadzirin and A. Nur (2017) Perancangan Sistem Monitoring Online Berbasis Motion Detector Menggunakan Rasberry PI. Pengenalan objek dengan melakukan pengenalan MAC address dari client sekaligus memberikan notifikasi melalui e-mail pengguna. [2]

c. S. Tri Utami, Bambang Eka Purnama (2014) Pembangunan Sistem Informasi Penjualan Obat Pada Apotek Punung. Sistem informasi data menggunakan Java netbeans yang memiliki fasilitas input data dan laporan [3]

d. J. Sarono (2014) Memaksimalkan Sistem Operasi Wndows Dengan Merubah Konfigurasi Registry yang dibackup dengan lebih mudah dengan menggunakan tool API khusus.[4]

e. W. Jusuf, Berlian, and Rosdiana (2014) Intruksi Bahasa Pemrograman ADT (Abtrack Data Type) Pada Virus dan Loop Batch. Virus yang trend sekarang rata-rata menggunakan intruksi perulangan batch, yang sering menggangu kinerja computer, dan penambahan data secara tidak diketahui kita karna kerja windows yang mengeset startup secara otomatis pada Task manajer.[5]

f. Archana et al., 2012 (Media Access Control Spoofing Techniques and its Counter Measures). Mac spoofing / pergantian alamat mac address sangat mungkin dilakukan karena IEEE 802.11 standart tidak menstandartkan adanya per-frame source authentication, yang dimana dapat menggunakan alamat mac address fake untuk terkoneksi dengan network.[6]

g. Computing, 2010 (Jamming and Anti-Jamming Techniques in Wireless Network Survey). Banyak jenis serangan jammer berbeda-beda di jaringan wireless, jenis serangan mempengaruhi dengan efek serangan jammer juga.[7]

h. Berdasarkan uraian di atas dapat disimpulkan bahwa penelitian ini merupakan penelitian baru (belum pernah ada di penelitian sebelumnya).

4. HASIL DAN PEMBAHASAN

a. Diagram blok

Secara garis besar perancangan penelitian dengan judul "Penanganan Wifi Jammer NodeMCU Esp8266 di Client Windows 10 dengan metode Mac spoofing" dapat dilihat dalam Gambar 5 diagram blok system berikut:

Gambar 5. Diagram Blok Sistem

Keterangan :

1) Client windows berfungsi sebagai user yang sedang mengakses internet ke AP dan mengalami serangan dari wifi jammer

2) Program mac spoofing berguna mengspoof mac address di client windows sehingga mendapatkan alamat mac baru guna terkoneksi kembali dengan access point

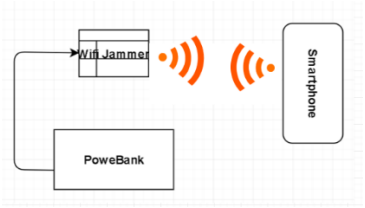
3) Access point sebagai sarana untuk koneksi internet dan sebagai alat untuk terhubungnya client windows ke internet.

b. Pembahasan Hasil Penelitian

Pembahasan hasil penelitian meliputi skema wifi jammer, pengujian wifi jammer, dan pengujian program. Maka dapat dilihat proses dari awal dan hasil serta perbedaan yang terjadi.

1) Skema Menjalankan wifi jammer

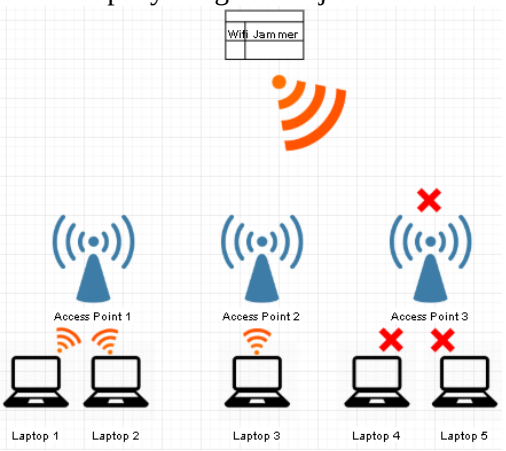
Merupakan skema yang menggambarkan menjalankan wifi jammer mulai dari menghidupkan dengan sumber tegangan (power bank) dilanjutkan dengan menghubungkan smartphone ke wifi jammer via wifi, smartphone digunakan untuk mengoperasikan wifi jammer, skema menjalankan wifi jammer ada di Gambar 6 berikut.



Gambar 6. Skema menjalankan wifi jammer

2) Skema Penyerangan wifi jammer

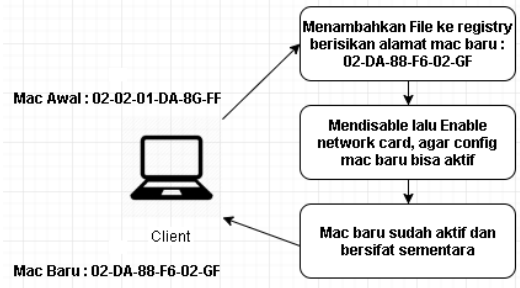
Wifi jammer yang sudah di operasikan dengan smartphone memulai serangan dengan melakukan scan Access Point(AP), setelah memilih AP yang akan di serang, wifi jammer melakukan scan ulang untuk melakukan scan client yang terkoneksi dengan AP yang sudah dipilih tersebut. Dan terakhir wifi jammer melakukan serangan ke client berdasarkan mac address tiap client. Gambar 6 merupakan skema dari penyerangan wifi jammer



Gambar 7. Skema penyerangan wifi jammer

3) Skema Client Melakukan MacSpoofing

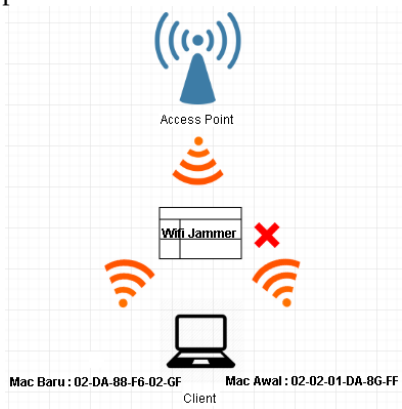
Melakukan Mac spoofing secara simple adalah dengan mengubah alamat mac addressdengan cara menambahkan file registry baru berisikan alamat mac yang ingin di pakai, agar mac baru bisa aktif client harus mematikan lalu menghidupkan network card dengan program semua bisa dilakukan secara otomatis. Barikut gambaran dari skema client melakukan mac spoofing di Gambar 7.



Gambar 8. Skema client melakukan mac spoofing

4) Skema Client Mendapatkan Koneksi Kembali

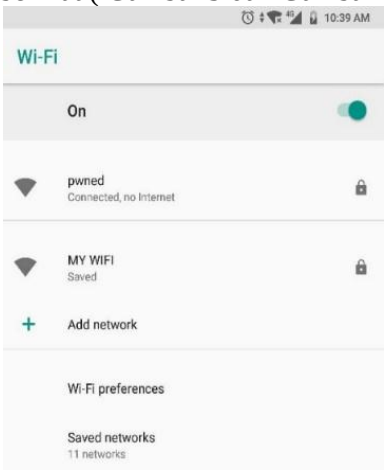
Client yang sudah melakukan mac spoofing maka secara tidak langsung Access point(AP) mengganggapnya sebagai client baru, dikarenakan memiliki mac addressyang berbeda, sehingga client dengan mudah bisa terkoneksi kembali dengan AP dan terhindar dari serangan wifi jammer karena wifi jammer menyerang alamat mac addressclient yang lama. Berikut Gambar 8, skema client mendapatkan koneksi kembali.



Gambar 9. Skema client mendapatkan koneksi kembali

5) Pengujian Wifi Jammer

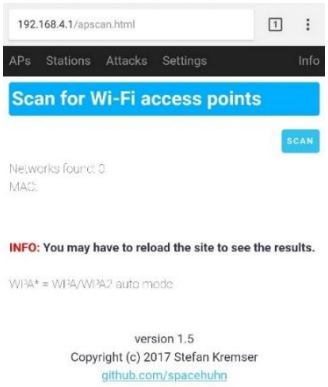
Pengujian bisa dilakukan setelah smartphone terkoneksi ke wifi jammer esp8266 via wifi, dan jika sudah terkoneksi smartphone bisa mengakses ip local dari esp8266 yaitu (192.168.4.1), seperti gambar di bawah berikut (Gambar 9 dan Gambar 10)



Gambar 10. Tersambung dengan ESP8266

Gambar 11. Membuka IP Local ESP8266

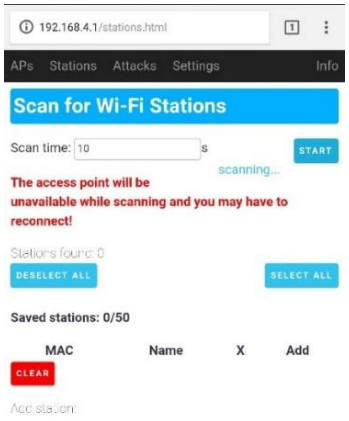
Setelah berhasil membuka ip local dari esp8266, selanjutnya smartphone digunakan untuk melakukan perintah scan access point dan memilih access point yang akan diserang client nya oleh esp8266. Berikut digambarkan pada Gambar 11 dan Gambar 12.



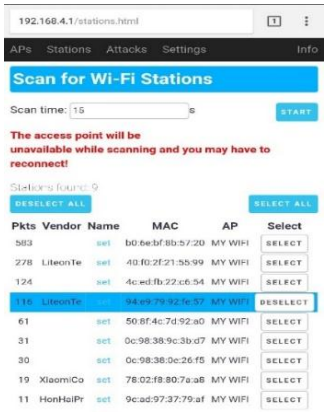
Gambar 12. Scan Access Point

Gambar 13. Memilih Access Point

Setelah memilih wifi yang di jadikan target selanjutnya adalah esp8266 menscan client target yang ada di jaringan wifi tersebut, proses scan perlu waktu 10-15 detik kemudian esp8266 akan menampilkan client yang tersedia untuk di serang di jaringan wifi yang di pilih seperti pada Gambar 13 dan Gambar 14.



Gambar 14. Scan Client



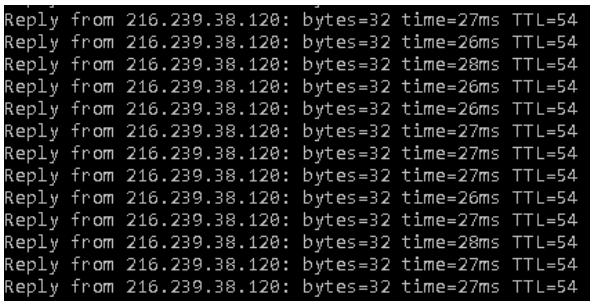
Gambar 15. Memilih Client

Kemudian setelah memilih client yang ingin diserang esp8266 siap melakukan jammer ke client wifi yang sudah di pilih, seperti pada Gambar 15 di bawah ini.

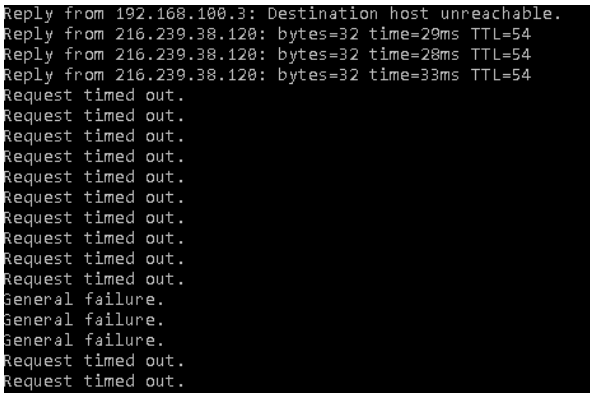
Gambar 16. Melakukan serangan ke client

Berdasarkan pengujian wifi jammer di atas dapat disimpulkan bahwa wifi jammer dapat memutus koneksi antara client dengan access point secara spontan, serta dapat dilihat perbedaan saat client sebelum dan sesudah

terkena serangan wifi jammer tersebut yang ditampilkan oleh Gambar 16 dan Gambar 17 di bawah ini.



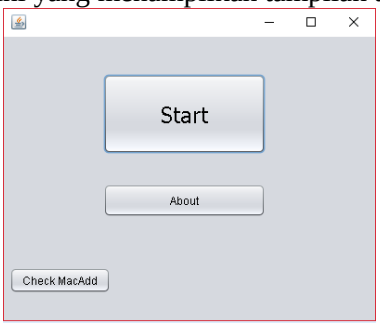
Gambar 17. Koneksi ping awal



Gambar 18. Koneksi RTO

6) Pengujian Program

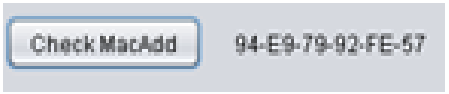
Program ini memiliki 2 tampilan utama yang merupakan 1 tampilan awal dan 1 tampilan utama program, seperti Gambar 18 di bawah ini yang menampilkan tampilan awal:



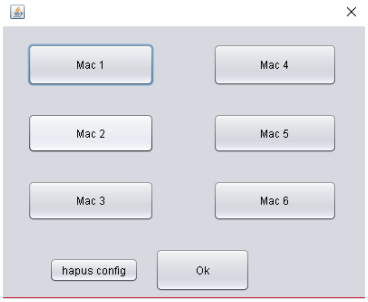
Gambar 19. Tampilan awal

Tampilan awal saat program dijalankan yang terdapat pilihan untuk menjalankan program utama, tentang, dan cek mac address. Ketiga tombol memiliki fungsinya masing-masing, tombol start untuk memulai program dan membuka tambilan utama, tombol about untuk melihat profile dan tombol check macadd untuk melihat alamat mac address yang sedang aktif.

Tampilan dari Gambar 19 adalah tampilan setelah tombol checkmac diklik, dan mac awal nya adalah 94:E9:79:92:FE:57. Program ini menampilkan mac address yang aktif dengan cara mengconvert dari ip address yang sedang aktif untuk di jadikan alamat mac address.



Gambar 20. Tampilan check my address



Gambar 21. Tampilan utama

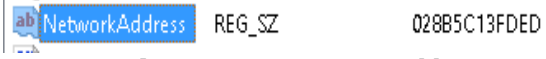
Pada Gambar 20 terdapat beberapa pilihan config mac address yang bisa di pilih dan juga ada tombol untuk hapus config berguna untuk mengembalikan alamat mac asli client, dan tombol ok untuk finish setelah memilih config mac address.

Perubahan mac address bisa dilihat setelah kita memilih config mac yang akan di jalankan dan mengklik tombol oke, untuk mengeceknya dengan tombol check mac address seperti pada Gambar 21 berikut

Gambar 22. Mac address baru

Setelah config berhasil terimport dan sudah menekan tombol ok, maka mac address baru sudah terpasang, dan dilihat pada pengecekan mac pada tombol checkmac, mac address sudah berubah sesuai config yang sudah di pilih.

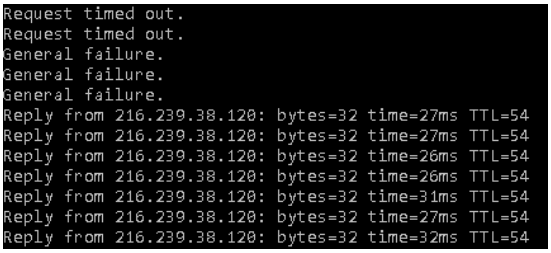
Saat pemilihan config mac address program otomatis melakukan import file registry ke dalam regedit, file inilah yang merupakan config dari mac address tersebut seperti pada Gambar 22 di bawah ini



Gambar 23. Registry mac address

Setelah program berhasil merubah alamat mac address secara langsung client bisa terkoneksi kembali ke Access Point(AP) hal ini dibuktikan dengan ping di cmd yang kembali

lagi ke reply dari RTO, seperti pada gambar 23 di bawah ini.



Gambar 24. Koneksi kembali normal

c. Hasil Pengujian

1) Pengujian BlackBox

Pada pengujian sistem digunakan metode black box. Metode ini dilakukan dengan cara mengevaluasi hasil program apakah sudah layak atau belum. Pengujian dilakukan dengan cara mengetahui hasil dari masukan dan keluaran. Misalnya keluaran dari sistem sudah sesuai dengan masukan maka sistem dikatakan lolos uji. Dengan kata lain metode black box adalah pengujian fungsionalitas sistem. Berikut hasil pengujian dengan metode black box yang akan di tunjukan pada tabel.

Tabel 1. Pengujian black box config mac address 1

Kondisi Awal	Client terserang wifi jammer dengan mac awal : 94-E9-79-92-FE-57
Data Program	File registry dengam alamat mac : 02-8B-5C-13-FD-ED
Yang Diharapkan	Program bisa melakukan mac spoofing dari mac address lama ke mac address baru dengan akurat sesuai dengan inputnya
Pengamatan	Program berhasil mengganti alamat mac address dari : 94-E9-79-92-FE-57 ke : 02-8B-5C-13-FD-ED dan sekaligus client bisa tersambung kembali ke AP
Kesimpulan	Lolos Uji

Program sukses melakukan mac spoofing dari mac awal ke config mac baru.

Tabel 2. Pengujian black box config mac address 2

Kondisi Awal	Client terserang wifi jammer dengan mac awal : 02-8B-5C-13-FD-ED
Data Program	File registry dengam alamat mac : 02-21-60-5F-88-08
Yang Diharapkan	Program bisa melakukan mac spoofing dari mac address lama ke mac address baru dengan akurat sesuai dengan inputnya
Pengamatan	Program berhasil mengganti alamat mac address dari : 02-8B-5C-13-FD-ED ke : 02-21-60-5F-88-08 dan sekaligus client bisa tersambung kembali ke AP
Kesimpulan	Lolos Uji

Didalam pengujian ini wifi jammer melakukan serangan kembali ke client dengan config mac address 1 yang aktif, kemudian program berhasil melakukan mac spoofing lagi ke alamat mac config 2.

Tabel 3. Pengujian black box config mac address 3

Kondisi Awal	Client terserang wifi jammer dengan mac awal : 02-21-60-5F-88-08
Data Program	File registry dengam alamat mac :02-CD-45-A7-84-74
Yang Diharapkan	Program bisa melakukan mac spoofing dari mac address lama ke mac address baru dengan akurat sesuai dengan inputnya
Pengamatan	Program berhasil mengganti alamat mac address dari : 02-21-60-5F-88-08ke : 02-CD-45-A7-84-74 dan sekaligus client bisa tersambung kembali ke AP
Kesimpulan	Lolos Uji

Pengujian ini sebenarnya hanya mengulang perintah pertama, tetapi program

melakukan import dengan config yang berbeda, sehingga config yang lama akan teredit dan digantikan config yang baru secara otomatis setelah perintah dijalankan.

Tabel 4. Pengujian black box config mac address 4

Kondisi Awal	Client terserang wifi jammer dengan mac awal :02-CD-45-A7-84-74
Data Program	File registry dengam alamat mac : 02-90-82-7E-2E-5E
Yang Diharapkan	Program bisa melakukan mac spoofing dari mac address lama ke mac address baru dengan akurat sesuai dengan inputnya
Pengamatan	Program berhasil mengganti alamat mac address dari : 02-CD-45-A7-84-74 ke : 02-90-82-7E-2E-5E dan sekaligus client bisa tersambung kembali ke AP
Kesimpulan	Lolos Uji

Tabel 5. Pengujian black box menghapus config mac address

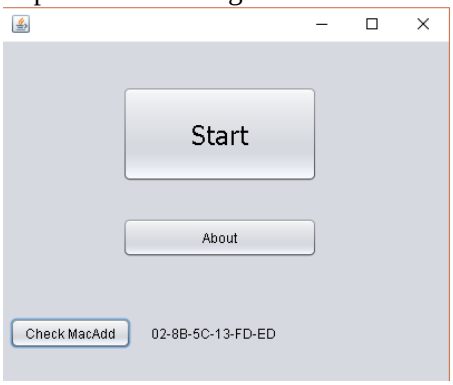
Kondisi Awal	Client terserang wifi jammer dengan mac awal : 02-90-82-7E-2E-5E
Data Program	File registry dengam alamat mac kosong : -
Yang Diharapkan	Program bisa melakukan mac spoofing dari mac address lama ke mac address baru dengan akurat sesuai dengan inputnya
Pengamatan	Program berhasil mengembalikan alamat mac address ke alamat semulanya dengan inputan registry kosong
Kesimpulan	Lolos Uji

Pengujian ini berhasil dengan cara menimpa file config mac address yang sudah di pilih oleh user dengan mac config kosong, sehingga config yang sedang berjalan bisa netral (dihapus). Berdasarkan hasil pengujian dengan metode Black box beserta beberapa data program, maka didapatkan kesimpulan bahwa sistem dapat dikatakan lolos uji. Melihat dan mengamati hasil dari fungsi – fungsi yang bekerja dengan baik dan sesuai perkiraan serta harapan. Hasil dari data sesuai dengan output yang diharapkan.

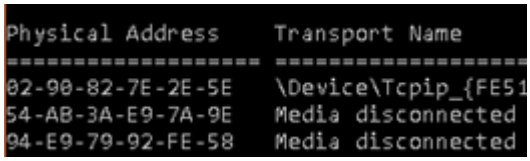
2) Pengujian Validasi

a) Uji Validasi Client berganti Mac Address

Pada uji validasi ini di lakukan cek validasi bahwa program berhasil mengganti alamat mac address baru dan dilakukan pengecekan melalui cmd bahwa client sudah berganti alamat mac address sesuai dengan inputan program. Uji validasi ini dibuktikan gambar yang menampilkan perbandingan alamat mac address di program dan di cmd, jika sama menandakan uji validasi berhasil. Gambar 24 dan Gambar 25 di bawah ini menampilkan dari config mac 1

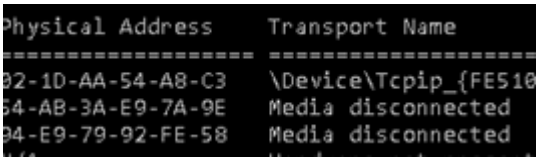


Gambar 25. Mac config 1 di program

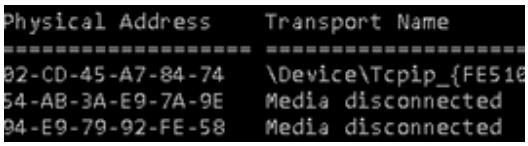


Gambar 26. mac config 1 di cmd

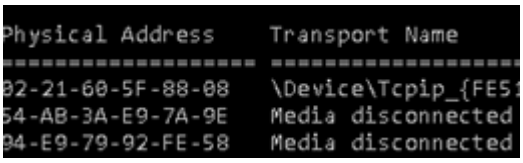
Dalam uji validasi ini dilakukan validasi pada semua config mac sehingga ditampilkan dalam Gambar 26, 27, 28, 29, adalah config mac di cmd.



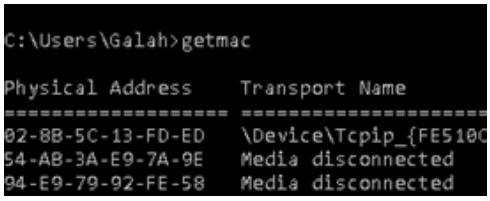
Gambar 27. mac config 2 di cmd



Gambar 28. mac config 3 di cmd



Gambar 29. mac config 4 di cmd



Gambar 30. mac config 5 di cmd

Berdasarkan gambar di atas dapat diambil kesimpulan bahwa uji validasi mac address berhasil lolos uji dikarenakan data yang ada pada program sesuai dengan data yang ditampilkan oleh cmd.

b) Pengujian berbeda client

Pada pengujian ini peneliti melakukan beberapa percobaan dengan berbeda client bertujuan untuk mengetahui perbedaan hasil apa saja dengan client peneliti, pengujian dilakukan ke 10 client yang berbeda versi windows, berbeda wifi card vendor dan hasil dari percobaan ini berupa tabel yang berisi perbedaan antara client peneliti dan client lain.Ditampilkan dalam tabel 6 dibawah ini.

Tabel 6. Pengujian berbeda client

Windows	Wifi Card	Directory Sub Registry	Hasil Program
Windows 10	Qualcomm Atheros 9377	{4d36e972-e325-11ce-bfc1-08002be10318}\0001	Berhasil
Windows 7	Qualcomm Wireless 9092	{4d36e972-e325-11ce-bfc1-08002be10318}\0000	Berhasil (dengan merubah script registry)
Windows 8	Qualcomm Atheros 9485	{4d36e972-e325-11ce-bfc1-08002be10318}\0001	Berhasil
Windows 10	Realtek 8821	{4d36e972-e325-11ce-bfc1-08002be10318}\0001	Berhasil
Windows 10	Realtek 8723	{4d36e972-e325-11ce-bfc1-08002be10318}\0001	Berhasil
Windows 10	Qualcomm Atheros 9285	{4d36e972-e325-11ce-bfc1-08002be10318}\0001	Berhasil
Windows 8	Qualcomm Atheros 9377	{4d36e972-e325-11ce-bfc1-08002be10318}\0001	Berhasil
Windows 8	Qualcomm Atheros956 X	{4d36e972-e325-11ce-bfc1-08002be10318}\0001	Berhasil
Windows 10	Qualcomm Atheros 9485	{4d36e972-e325-11ce-bfc1-08002be10318}\0001	Berhasil
Windows 10	Realtek 8192	{4d36e972-e325-11ce-bfc1-08002be10318}\0001	Berhasil

Berdasarkan tabel diatas dapat disimpulkan bahwa program bisa dijalankan disemua versi windows dengan berbeda operating sistem dan vendor driver, akan tetapi dengan syarat subkey directory registry adalah 0001, jika berbeda maka program jika ingin berhasil dijalankan makan harus ada perubahan scrip pada bagian program file registry. Directory sub registry yang ada pada tabel adalah difolder Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\ (dilanjut dalam tabel 6).

c) Pengujian berbeda jarak

Pada pengujian ini peneliti melakukan beberapa percobaan jarak dengan 2 jenis

NodeMCU yang dipakai dalam penelitian ini yaitu v0.9 dan v1.0, tujuan dari pengujian ini adalah untuk mengetahui batas jarak yang bisa di capai wifi jammer untuk menyerang dan untuk mengetahui perbedaan apa yang ada di v0.9 dan v1.0 dalam hal jarak penyerangan, hasil dari penelitian ini adalah tabel 7 di bawah ini. Berdasarkan tabel 7 di bawah dapat disimpulkan bahwa V1.0 lebih baik dalam mengkap sinyal di rentan 10-15Meter dari AP (Access Point). sinyal yang dimaksut adalah sinyal saat wifi jammer NodeMCU melakukan scan AP di sekitarnya, dalam kondisi sinyal hijau dan kuning penyerangan wifi jammer berjalan lancar tanpa adanya masalah, tetapi dalam kondisi sinyal merah penyerangan wifi jammer sering mengalami putus ditengah karena kondisi sinyal yang sangat tidak stabil.

5. PENUTUP

a. Kesimpulan

Berdasarkan masalah ada dalam penelitian ini yaitu penyerangan wifi jammer NodeMCU esp8266 di client

Tabel 7. Pengujian Jarak

Versi Node MCU	Jarak				
	<5M	<10M	15M	20M	25M
V0.9	Sinyal Hijau	Sinyal Hijau	Sinyal Kuning	Sinyal Kuning	Sinyal Merah
V1.0	Sinyal Hijau	Sinyal Hijau	Sinyal Hijau	Sinyal Kuning	Sinyal Merah

Windows 10 maka solusi dari masalah tersebut adalah client melakukan mac spoofing sebagai cara penanganan jika terserang wifi jammer ini, maka dapat disimpulkan dari penelitian ini adalah sebagai berikut:

1) Program yang dibuat bisa untuk menangani client dari serangan wifi jammer NodeMCU Esp8266

2) Hasil dari 10 percobaan terhadap berbagai client adalah program bisa di pakai di semua versi windows akan tetapi pada windows 7 perlu adanya perubahan script dikarenakan perbedaan folder pada registry nya.

3) Hasil dari percobaan dari aplikasi yang telah digunakan dapat merubah mac address secara berkali-kali

4) Program yang dibuat dapat menampilkan mac address pada windows 10 dengan akurat

5) Hasil dari percobaan dari aplikasi yang telah digunakan dapat merubah mac address secara berkali-kali

6) Hasil dari percobaan jarak wifi jammer nodeMCU V1.0 lebih baik dalam menangkap sinyal AP(Access Point) daripada V0.9 di jarak 15M, sedangkan jika sinyal dalam kondisi merah wifi jammer cenderung gagal dalam melakukan serangan.

b. Saran

Adapun saran dari "Penanganan wifi jammer nodeMCU esp8266 di client windows 10 dengan metode mac spoofing" adalah sebagai berikut :

1) Program bisa menerima inputan mac address dari client dan memprosesnya

2) Program bisa berjalan di sistem operasi selain windows

6. REFERENSI

[1] F. Eka, "Kontrol dan Monitoring Smarthome dengan Modul esp8266 serta Server Thinkspeak," 2017.

[2] M. Nadzirin and a. Nur, "Perancangan Sistem Monitoring Online Berbasis Motion Detector," pp. 31–36, 2017.

[3] S. Tri Utami, Bambang Eka Purnama, "Pembangunan sistem informasi penjualan obat pada apotek punung naskah publikasi," IJCSS-Indonesian J. Comput. Sci. UNSA, vol. 4, no. Bisnis Intelijen, pp. 1–16, 2014.

[4] J. Sarono, "Memaksimalkan Sistem Operasi Windows Dengan Merubah Konfigurasi Registry," pp. 23–30, 2014.

[5] W. Jusuf, Berlian, and Rosdiana, "Instruksi Bahasa Pemrograman Adt (Abstract Data Type) Pada Virus Dan Loop Batch," J. Media Infotama, vol. 9, no. 2, pp. 64–77, 2014.

[6] H. Archana, V. Gauri, and H. Arvind, "Media Access Control Spoofing Techniques and its Counter Measures," Int. J. Sci. Eng. Res., vol. 2, no. 6, pp. 1–5, 2012.

[7] U. Computing, “Jamming and Anti-jamming Techniques in Wireless Networks : A Survey,” vol. x, no. x, 2010.