e-ISSN: 2655-1438
p-ISSN: 2655-1632

Analisis dan Pengujian Sistem Keamanan pada Jaringan WIFI

Ifan Hidayat [1)], Ria Andriani [2)], Cessaricki Yudi Kurniadi [3)], Ari Ardianto [4)]

[1,2,3)] *Teknik Informatika Universitas AMIKOM Yogyakarta*
email : ifan.2000@students.amikom.ac.id [1)], ria.amikom.ac.id [2)], cessaricki.k@students.amikom.ac.id [3)]
ari.ardianto@students.amikom.ac.id [4)]

Abstraksi

Pada perkembangan teknologi, kehidupan manisia saat ini sulit di pisah dengan teknologi informasi dan komunikasi. Contoh dari teknologi komunikasi dan informasi adalah jaringan wireless. Tidak bisa kita pungkiri hampir di semua tempat ada wireless, misal di kantor, sekolah, kedai, dan laininya. Terkadang banyak orang tidak menyadar bahwa kerentanan keamanan data pada jaringan sangat rawan. Pada proses bertukarnya data banyak celah di jaringan wireless itu.. Peneliti ingin membantu untuk beberapa cara untuk meminimalisir terjadinya kerentanan data keamanan hal itu, terutama pada sistem keamanan wireless. Pada jaringan wireless ada 3 tols sitem keamananya, yaitu WPA, WPA2 serta MAC Filtering. Pada keamanan jaringan wireless menggunakan WPA yaitu mengunakan password default. Keamanan ini sangat rentang, karena WPA menggunkan password default. Pada jaringan wireless menggunakan sitem keamanan WPA2 in dimana menggunakan password yang telah terenkripsi. Sedangkan MAC Filterng ini yatu. Membatasi mana user yang terdaftar dan dimana user yang tidak terdaftar pada jaringan wareless. Kami peneliti juga memberi tahu salah satu cara orang yang tidak bertanggung jawab bagaimana cara masuk kesebuah jaringan wareless, dengan cara menggunakan Airgeddon.

Kata Kunci : *Wareless, Keamanan, Data.*

Abstract

In the development of technology, the current sweet life is difficult to separate from information and communication technology. An example of communication and information technology is a wareless network. We can not deny that almost everywhere there is wareless, for example in offices, schools, shops, and others. Sometimes many people don't realize that data security vulnerabilities on networks are very vulnerable. In the process of exchanging data, there are many gaps in the wareless network. Researchers want to help in several ways to minimize the occurrence of data security vulnerabilities, especially in wareless security systems. In wareless networks there are 3 security system tols, namely WPA, WPA2 and MAC Filtering. In the wareless network security using WPA that is using the default password. This security is very wide range, because WPA uses the default password. On wareless networks use the WPA2 in security system which uses an encrypted password. Whereas MAC Filterng is correct. Restrict which users are registered and where users are not registered on a wareless network. We researchers also tell one of the ways irresponsible people enter a wareless network, by using Airgeddon.

Keywords : *Wareless, Security, Data*

Pendahuluan

Perkembangan teknologi saat ini sangat pesat, terutama pada teknologi informasi dan komunikasi yang terbarukan. Telepon seluler (*handphone*), komputer, laptop, kebanyakan menggunakan *wireless*. Jaringan *wireless* mengimplementasikan jaringan lokal yang WLAN (*Wireless Local Area Network*). Jaringan *wireless* teknologi saling bertukar data menggunakan gelombang radio (secara nirkabel) dengan memanfaatkan berbagai peralatan elektronik. Diperlukan peralatan elektronik di dalamnya, misal komputer, smartphone dan lainya. hampir semua tempat ada wifinya. warung makan, kosan, tempat kerja dan tempat lainnya. Setiap perangkat tersebut saling bertukar data satu sama lain. pada proses pengiriman data melewati beberapa terminal. Maka kerentanan data terhadap keamanan sangat tinggi. Banyak berbagai cara untuk mengamankan proses saling bertukarnya data seperti

adanya user, nah dari itu memberikan celah lagi terhadap keamanan *wireless* kepada penyerang, sehingga mengetahui *password* keamanan *wireless* pada user yang tersambung pada jaringan tersebut. Pada jaringan *wireless* ada beberapa kelemahannya, terletak pada empat layer. Dimana empat lapis layer di mana keempat layer merupakan proses terjadinya komunikasi data pada jaringan *wireless*. Keempat lapisan tersebut adalah fisik, lapisan jaringan, lapis *user* dan lapisan aplikasi.

Keamanan pada jaringan sangat penting terutama pada *wireless* yang di bahas kali ini, karena celah keamanan selalu di ekskploitasi oleh pihak yang tidak bertanggung jawab. Oleh sebab itu kami ingin menganalisis keamanan jaringan pada wirelass, dimana yang menjadi celah pada keamanan WiFi.

Rumusan Masalah

Berikut Rumusan Masalah dari jurnal ini:

1. Apa itu WPA2?
2. Apa saja jenis enkripsi WPA2?
3. Apa itu WPS?
4. Bagaimana cara meningkatkan keamanan pada jaringan WIFI?
5. Bagaimana cara mencegah serangan pada serangan pada jaringan WIFI?

Batasan Masalah

Pada jaringan *wireless* ini mempunyai batasannya. Analisis ini lebih condong terhadap WPA2 (Wi-Fi Protected Access), peneliti memberi batasan maslah agar penelitian hasilnya lebih maksimal dari apa yang di harapkan. Adapun batasan masalah nya:

1. Penelitian ini hanya untuk WPA2, yang personal
2. Penelitian ini hanya menggunkan *wireless* di rumah.
3. Metode dalam penelitian ini menggunakan methode kuantitatif.

Maksud dan Tujuan Penelitian

Berikut adalah tujuan penelitian ini:

1. Mengetahui sistem kemanan jaringan *wireless* , dan cara kerja keamanan tersebut.
2. Mengptimalisasi keamanan jaringan *wireless.*

Tinjauan Pustaka

Pada penelitian yang dilakukan oleh Lawrence and Lawrence (2004). Pada penelitain ini menjelaskan tentang pengaruh warchalking dan wardriving dalam konteks keamanan. Dalam penelitian ini memberikan pendapat tentang kebijakan bagi teknisi, ilmuwan, dsan pengambilan kebijakan dalam pemerintahan di negaranya. penelitian ini mengembangkan sebuah *framework.* Nah *framework* ini berada di perusahaan *mobile phone* yang bertujuan untuk memastikan bahwa suatu perusahaan itu berada dalam wilayah hukum dan jaringan untuk menjaga keamanan jaringan suatu perusahaan itu [1].

Pada penelitian yang di lakukan oleh Sonny Rumalutur(2014) yang berjudul *Analsis Keamanan Jaringan Wireleess Lan (Wlan).* Peneliti menganalisa keamanan *wireless* di perusahaan PT. PLN (Persero) Wilayah P2B Area Sorong, peneliti mengatasi kelemahan pada integritas data dan ketersediaan pada sistem perusahaan tersebut. Dan juga peneliti melakukan percobaan untuk membuktikan
kelemahan protokol WPA. Peneliti tidak hanya menganalisa keamanan WPA saja tapi juga *web proxy* di perushaan tersebut. Peneliti berhasil menemukan kelemahan jaringan *wireless* pada perusahaan itu[2].

Pada penelitian yang dikukan oleh Marti Widya Sari(2017) yang bejudul *Analsis keamanan jaringan wi-fi Menggunakan Metode Signal Scanning.* Penulis meneliti di Fakultas Teknik Universitas PGRI Yogyakarta. Penulis menganalisa banyaknya device yang dibutuhkan, tempat (gedung), dan juga penulis juga menggunakan software inSSIDer untuk *scanning* sinyal *access point.* Kegunaan dari SSID itu *scanning* kekuatan sinyal dan keamanan jaringan. *Open Scurity* artinya user bisa menggunakan login pada jaringan itu menggunakan *user* dan *password.* Jadi penulis berhasil menganalisa suatu jaringan dari kecepan frekuensi serta keamanan itu sendiri[3].

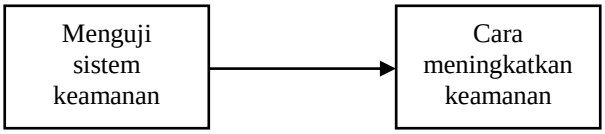
Pada penelitian yang dilakukan oleh Heather, D. Lane. 2009 tentang bagaimana cara untuk mengetahui *password* dari WPA2, WPA2-PSK penyerang harus memerlukan pengguna(user) yang sudah tersambung melalui jaringan *wireless* itu sendiri dengan menggunakan tool Fluxion. Pada pengujian SSID palsu attacker membuat sebuah SSID yang berbeda yang hampir sama dengan SSID asli, yang menjadi pembeda pada SSID adalah pada SSID asli memeliki pengaman WPA2/WPA2SK. sedangkan yang palsu bersifat open, jadi user tidak bisa mebedakan mana SSID yang asli dan yang palsu. Maka dari itu attacker akan mudah mendapatkan *password* user dan memasukkan password dari SSID yang asli yang sudah dibuat oleh tool WiFiPhiser. Dalam tahapan mengetahui *password* penyerang masih membutuhkan *user* yang terhubung ke jaringan WiFi, bukan melakukan proses mendapatkan *password* secara individu. Jadi itulah celah untuk mengetahui keamanan password dari WPA2, WPA2-PSK dengan menggunakan tools Fluxion dan WiFiPhiser[4].

e-ISSN: 2655-1438
p-ISSN: 2655-1632

Pada penelitian yang dilakukan oleh Muis Rajab dari Universitas Islam Negeri Jakarta yang berjudul tentang *Analisa dan Perancangan Wireless LAN Security menggunakan WPA2-RADIUS*. Dari hasil Implementasi Pengujian dan pengamatan dilapangan. Sistem keamaan WPA2-RADIUS ini bisa ditarik pengertian. Sistem keamana LAN ini bisa berjalan dengan baik. Terlebih dahulu konfigurasi client yang akan melakukan koneksi. Pada sistem ini berjalan dengan lancar. Pada sistem keamanan dapat membantu user dalama keamanan pada jaringan *wireless* yang lebih secure. Sehingga user yang terkonelsi dengan jarigan wireless menjadi lebih terkontrol, keamanan data sesuai prosedur perancang jaringan yang dinginkan. Meskipun ada celah dari sistem security pada jaringan pada radius pun bisa terdeteksi menggunakan aplikasi Nessus, jadi dapat dilakukan proses untuk patch dan update agar minim dan tidak membahayakan bagi keamanan itu sendiri. [5].

Pada penelitian yang dilakukan oleh Fakultas Teknik UHO di labolatorium Sistem Informasi dan *Programming* Jurusan Teknik Informatika tentang analisa keamanan jaringan *Wireless Local Area Network* dengan Metode Pada penelitian yang dilakukan oleh Fakultas Teknik UHO di labolatorium Sistem Informasi dan *Programming* Jurusan Teknik Informatika tentang analisa keamanan jaringan Wireless Local Area Network dengan Metode Penetration Testing (Cracking The Encryption, Bypassing WLAN Authentication, Attacking The Infrastructure dan MITM) menggunakan kali linux dapat di simpulkan bahwa keamanan yang dimiliki oleh Jaringan WLAN Masih memiliki banyak celah untuk dieksploitasi. Hal ini di buktikan dari penelitian ini dengan menggunakan 4 jenis serangan yang dilakukan dan hanya gagal pda serangan Cracking The Encryption. Jaringan Wlan belum bisa memberi keamanan pada user agar tidak dapat mendapatkan gangguan maupun penyadapan dari user lain saat mengakes layanan internet yang sama dan MITM) menggunakan kali linux dapat di simpulkan bahwa keamanan yang dimiliki oleh Jaringan WLAN Masih memiliki banyak celah untuk dieksploitasi. Hal ini di buktikan dari penelitian ini dengan menggunakan 4 jenis serangan yang dilakukan dan hanya gagal pda serangan Cracking The Encryption. Jaringan Wlan belum bisa memberi keamanan pada user agar tidak dapat mendapatkan gangguan maupun penyadapan dari user lain saat mengakes layanan internet yang sama[6].

Metode Penelitian



1. Menguji sistem keamanan
   a. Menggunakan Wifite
      Dengan menggunakan tool ini kita akan mencari manakah wifi yang menggunakan WPS.
   b. Menggunakan Airgeddon
      Dengan menggunakan tool ini kita akan mencoba mencari password wifi dengan memanfaatkan client yang terhubung pada jaringan.

2. Meningkatkan sistem keamanan
   a. Matikan pengaturan WPS pada router
      WPS sering menjadi ancaman serangan oleh karena itu kita matikan saja WPS
   b. Pilih jenis enkripsi WPA2
      Jenis enkripsi WPA2 juga berpengaruh terhadap keamanan *wareless* oleh karena itu kita tentukan jenis enkripsi dari WPA2
   c. Gunakan MAC filter
      Untuk mencegah serangan maka kita gunakan fitur mac filter untuk menentukan siapa saja yang dapat menggunakan WIFI
   d. Sembunyikan SSID WIFI
      Untuk mencegah adanya serangan kita bisa sembunyikan SSID *wareless* sehingga orang mengira tidak ada jaringan WIFI yang berada disekitar

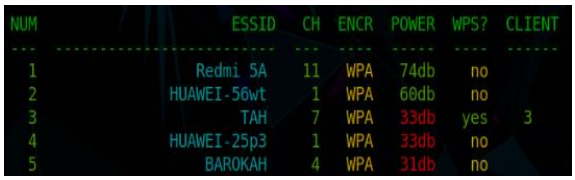
Hasil dan Pembahasan

Menguji sistem keamanan

Pengujian akan dimulai dengan mencari referensi tentang keamanan jaringan *wareless* lalu menyiapkan *hardware* dan *software* yang dibutuhkan untuk mengamati, menganalisa, serta menguji kemamanan sebuah jaringan *wareless.*
Untuk bagian *hardware***:**

1. Laptop dengan OS Linux
2. Wireless card dengan dukungan monitor
   Untuk bagian *software:*
1. Airgeddon
2. Wifite
3. Tool tambahan lain

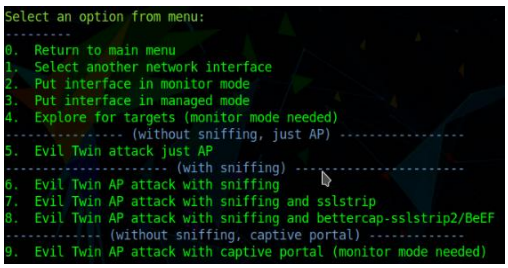
Langkah selanjutnya adalah memulai menganalisa jaringan *wareless* dengan menggunakan *Wifite*.



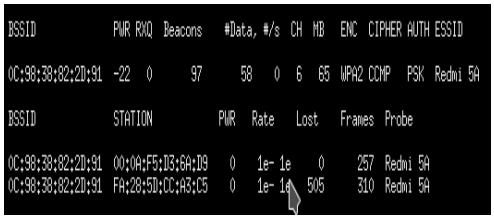
Terlihat pada bagian WPS ada yang menunjukan keterangan *"Yes" dan "No". Jika pada bagian WPS menunjukan* "Yes" artinya wifi tersebut mempunyai sebuah celah keamanan dengan memanfaatkan WPS untuk mengetahui key WPA2 dari jaringan tersebut.

Tahapan-Tahapan pengujian keamanan dengan menggunakan *Airgeddon*:

1. Mengkonfigurasi tool *Airgeddon* serta tool lain yang tersedia di ParrotSec untuk mempersiapkan proses pengujian

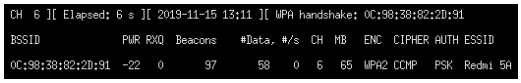


2. Mengecek apakah ada user yang menggunakan WIFI target.
3. Memutuskan koneksi user dengan *wareless* target



menggunakan metode *MDK4* pada *Airgeddon.*

4. Mengcapture (menangkap) handshake WPA2 dari user yang terputus dari jaringan untuk dijadikan sample Fake login dengan memanfaatkan SSID Palsu.



5. Membuat SSID cloning dan memutuskan koneksi user dari *wireless* sebenarnya dan memaksa user untuk tersambung ke SSID palsu buatan kita dan saat user sudah tersambung maka saat user akan menggunakan internet secara berkala user akan dialihkan ke halaman Fake login untuk dipaksa memasukan password WIFI.

6. Saat user belum memasukan password yang benar dari WIFI sebenarnya maka user akan terus dialihkan ke halaman Fake login

7. Setelah user memasukan password yang benar maka akan tampil pesan bahwa password yang dimasukan sudah benar.

8. Maka secara otomatis semua proses dari tool *Airgeddon* akan berhenti secara otomatis dan menampilkan password dari *wareless* target.

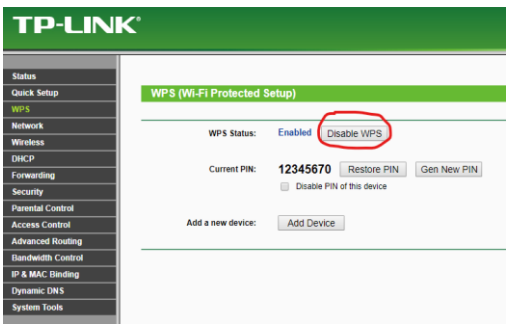
Meningkatkan sistem keamanan

Keamanan jaringan merupakan salah satu poin penting pada sebuah jaringan WIFI, karena semakin banyaknya kebutuhan koneksi internet membuat para penyedia layanan internet berbasis WIFI seperti Hotspot rumah ataupun Hotspot Warnet semakin waspada dengan adanya pembobolan pada jaringan WIFI. Salah satu cara mengamankan jaringan WIFI adalah dengan memanfaatkan keamanan WIFI yang sudah tersedia, jenisnya pun beragam contohnya WPA2. Istilah ini mungkin cukup asing bagi orang-orang yang belum mengetahuinya, sedangkan keamanan pada jaringan sangat diperlukan.

Karena itu untuk mengatasi masalah diatas kita dapat meningkatkan keamanan jaringan *wareless* dengan tahapan – tahapan berikut:

1. Pengaturan WPS

   WPS adalah singkatan dari *Wareless Protected Setup*. Ini merupakan sebuah sistem keamanan pada *wireless* yang berguna untuk menghubungkan router dengan perangkat penerima *wireless* agar menjadi lebih cepat dan mudah dengan menggunakan PIN.
   Namun dengan kemudahan itu juga terdapat ancaman karena biasanya pada pengaturan bawaan Router terdapat PIN default yang dapat dimanfaatkan sebagai celah keamanan oleh karena itu akan lebih baik jika WPS dimatikan saja. Sebagai contoh dibawah ini cara mematikan WPS pada Router TP-LINK TL-



e-ISSN: 2655-1438
p-ISSN: 2655-1632

WR841N masuk ke menu WPS > lalu pilih Disable WPS

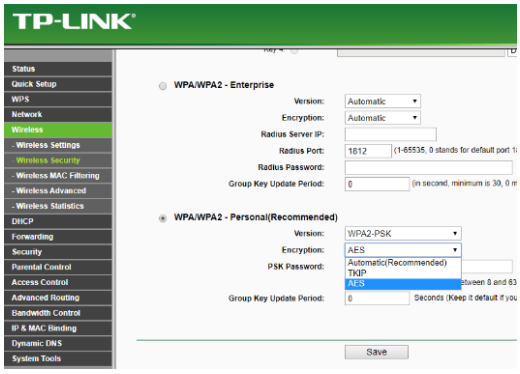
2. Pengaturan Enkripsi WPA2

Setiap router biasanya menyediakan beragam jenis enkripsi untuk mengamankan jaringan. Misalnya WPA2-PSK (TKIP), WPA2-PSK (AES), dan WPA2-PSK (Mixed).

TKIP merupakan standar enkripsi yang sudah ada lebih dulu yang bisa digunakan bersamaan dengan WPA2. Sedangkan AES adalah enkripsi terbaru dan merupakan solusi baru untuk mengamankan jaringan WIFI yang bisa digunakan bersamaan dengan WPA2.

Secara teknis, TKIP hampir mirip dengan WEP dan belakangan ini sudah mulai ditinggalkan karena dirasa kurang aman. Dengan kata lain, jika ada enkripsi selain TKIP lebih baik anda menggunakan itu, misalnya AES atau MIxed.

Pada pada Router TP-LINK TL-WR841N kita dapat memilih jenis enkripsi pada menu Wireless > Wireless Security



3. Penggunaan MAC Filtering

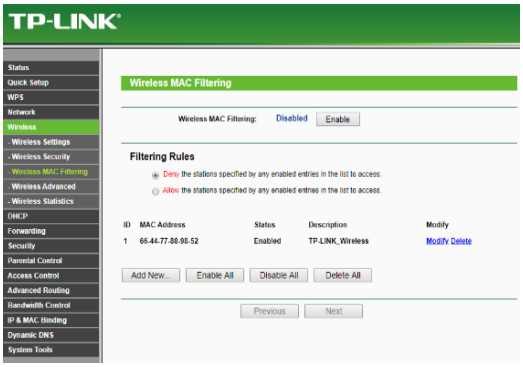
MAC Address Filtering merupakan metode filtering untuk membatasi hak akses dari MAC Address yang bersangkutan. Hampir setiap wireless access point maupun router di fasilitasi dengan keamanan MAC Filtering. MAC filters ini juga merupakan metode sistem keamanan yang baik dalam jaringan *wareless*.

MAC filter mempunyai 2 mode yaitu **allow** dan **deny**

Untuk allow berfungsi untuk mengecek perangkat mana yang bisa masuk ke dalam jaringan berdasarkan MAC Address. Bila tidak ada dalam daftar MAC yang diijinkan, maka perangkat tersebut tidak akan bisa masuk ke jaringan WIFI. Alamat MAC dari perangkat komputer ataupun gadget user akan dimasukan ke dalam daftar MAC yang diijinkan dahulu untuk bisa tersambung dengan jaringan WIFI.

Untuk deny berkebalikan dengan allow yaitu jika MAC ada didalam daftar maka perangkat tersebut tidak akan bisa masuk ataupun tersambung ke dalam jaringan WIFI.

Pada Router TP-LINK TL-WR841N kita dapat memilih jenis enkripsi pada menu Wireless > Wireless MAC Filtering



Kesimplan dan Saran

Berdadarkan penelitian yang telah dilakukan di atas. *Mengnalisa serta menguji keamanan pada jaringan wifi*, dapat disimpulkan bahwa:

1. Tahap pengujian jaringan dengan menggunkan *Airgeddon.* Yaitu untuk mengetahui *password* jaringan *wareless.*
2. Tahap peningkatan keamanan jaringan *wareless.* Yaitu penggunaan WPS, WPA2, dan MAC Filtering.
3. WPS (*Wareless Protected Setup)* adalah pengamanan jaringan yang menggunkan *password* secara default.
4. WPA2 adalah versi ke 2 dari WPA, perbedaan dari WPA2 dengan WPA yaitu *password* terencripsi.
5. MAC Filtering merupakan metode filtering untuk membatasi hak akses dari MAC Addess yang bersangkutaan. MAC Filtering ini mempunyai dua metode, allow dan deny. Dimana metode allow itu mana *ip address* yang boleh tersambung. Sedangkan allow, yaitu bila ip address tidak terdaftartidak akan bisa terhubung dengan jaringan *wifi* kita.

Saran

Adapun saran dari penelitian ini,yaitu diihrapkan untuk sebaiknya mematikan WPS agar meminimalisir celah pada *wireless.* Ini dapat menjadi evaluasi bagi para pengguna WPA pada *wireless*. Kami berharap kepada peneliti selanjutnya agar meneliti tentang jarinagn *wireless*, karena pada pada penelitian ini kurang maksimal dalam penelitian ini.

Daftar Pustaka

[1]Lawrence E, & Lawrence J. (2004). Threats to The Mobile Enterprise: *Jurisprudence Analysis of Wardriving and Warchalking*. IEEE Journal.

[2]Rumalutur S., (2014). Analsis Keamanan Jaringan Wireless LAN (WLAN) 13, 14.

[3]Sari W. M., Analisis Keamanan Jaringan WiFi Menggunakan Metode Scanning. 5,6.

[4]Rajab M., (2010). Analsis dan Perancangan Wireless Lan Security Menggunakan WPA2-Radius. *Skripsi Gelar Sarjana*. 130, 132

[5]Baihaqi, Yeni Y., Zulfan., (2017). Implementasi Keamanan WPA2-PSK Pada Jaringan WiFi. *Jurnal Serambi Engenering*. 252, 253.

[6]Bayu K. I., Yamin M., Aksara F. LM., (2017). Analisis Keamanan Jaringan WLAN dengan Metode Peneration Testing. 6, 7.