# Pengujian Celah Keamanan 5 Jenis Metode *Wireless* LAN *Security*

**Arini, MT, Muis Rajab**
Program Studi Teknik Informatika
Fakultas Sains Dan Teknologi
UIN Syarif Hidayatullah Jakarta
arinizoel@yahoo.com, muis.rajab@gmail.com

***Abstract— Wireless network offer many facilities and flexibility but to support them require high serious of security. Many types of Wireless LAN security mechanisms had implemented today such WEP (Wired Equivalent Privacy), WPA/WPA2 (Wi-Fi Protected Access), MAC Filtering, and Hidden SSID, or even used WPA2 combine with RADIUS. In this topic, we will look more depth the some weakness of the Wireless LAN (WLAN) security as the way to find the solution to obtain the security policy of our WLAN. By using some testing procedure and provided of the Open source tool, we found some weakness of security problem in WLAN.***

***Keywords :*** *Wireless LAN,* WEP (*Wired Equivalent Privacy*), WPA/WPA2 (*Wi-Fi Protected Access*), MAC *Filtering*, *Hidden* SSID, WPA2-RADIUS

## I. PENGANTAR

Teknologi *wireless* menawarkan beragam kemudahan, kebebasan, mobilitas dan fleksibilitas yang tinggi pada zaman yang serba cepat ini. Namun dibalik segala macam kelebihan yang ditawarkan tersebut, masalah keamanan pada jaringan *wireless* memerlukan perhatian yang lebih serius mengingat media transmisi data adalah udara yang bersifat *broadcast*.

Sistem keamanan yang paling umum diterapkan pada *wireless* LAN adalah dengan metode enkripsi, yaitu WEP (*Wired Equivalent Privacy*) dan WPA/WPA2 (*Wi-Fi Protected Access*). Ada pula yang menggunakan metode MAC *Filtering*, atau bahkan hanya mengandalkan SSID yang disembunyikan (*Hidden* SSID).

Jenis keamanan tersebut masing-masing memiliki kelemahan yang rentan dan memerlukan pengujian untuk membuktikannya. Hal ini diperlukan agar terhindar dari penggunaan keamanan yang lemah.

Dari hasil studi pustaka yang dilakukan, sistem keamanan *wireless* yang benar-benar mampu memberikan keamanan dengan kuat adalah dengan menggunakan keamanan dengan level *enterprise*. Yaitu dengan mengaplikasikan WPA/WPA2 dengan teknologi IEEE 802.1x. Pada sistem keamanan ini, proses autentikasi dilakukan oleh sebuah *server* khusus, yaitu RADIUS (*Remote Authentication Dial In User Service*), dengan menggunakan *username* dan *password*. Sistem keamanan ini sering juga disebut dengan WPA2-RADIUS.

## II. TEORI PENUNJANG

### A. *Hidden SSID*

Secara *default*, *access point* mem-*broadcast* SSID setiap beberapa detik dalam *beacon frame* untuk memudahkan bagi *authorized user* untuk mencari jaringan yang benar. Akan tetapi hal ini juga memudahkan bagi *unauthorized user* untuk mendapatkan nama jaringan tersebut.

Rata-rata *access point* menawarkan modus "rahasia", yaitu modus dimana *access point* akan menyembunyikan nama jaringan SSID-nya sehingga tidak akan terdeteksi oleh *wireless scanner* seperti NetStumbler.

Namun sayangnya hal ini tidak berlaku untuk aplikasi yang menggunakan metode *passive scanning* seperti Kismet. Dimana aplikasi ini akan menangkap semua paket data yang dikirim termasuk SSID yang disembunyikan.

### B. *MAC Filtering*

Pemfilteran MAC *address* (MAC *Filtering*) merupakan pemfilteran di atas standar 802.11b untuk mengamankan jaringan. MAC *address* dari *card* jaringan adalah bilangan *hexadecimal* 12 digit yang unik satu sama lain. Karena masing-masing *card wireless* Ethernet memiliki MAC *address*-nya sendiri, maka jika Anda hendak membatasi akses ke AP hanya pada MAC *address* dari peranti yang telah diotorisasikan tersebut, Anda dapat dengan mudah mengeluarkan tiap orang yang tidak berada pada jaringan Anda.

Akan tetapi, pemfilteran MAC address tidak seluruhnya aman dan jika Anda semata-mata mengandalkan pemfilteran MAC *address*, Anda akan mendapatkan kegagalan [1].

### C. *WEP (Wired Equivalent Privacy)*

WEP (*Wired Equivalent Privacy*) adalah suatu metode pengamanan jaringan *wireless*, disebut juga

dengan *Shared Key Authentication*. Enkripsi WEP menggunakan kunci yang dimasukkan (oleh administrator) ke *client* maupun *access point*. Kunci ini harus cocok dari yang diberikan *access point* ke *client*, dengan yang dimasukkan *client* untuk autentikasi menuju *access point*.

Menurut Gunawan (2004), Komunikasi Data via IEEE 802.11, *Shared Key Authentication* kelihatannya lebih aman dari dari pada *Open System Authentication*, namun pada kenyataannya tidak. *Shared Key* malah membuka pintu bagi penyusup atau *cracker*. Penting untuk dimengerti dua jalan yang digunakan oleh WEP. WEP bisa digunakan untuk memverifikasi identitas *client* selama proses *shared key* dari authentikasi, tapi juga bisa digunakan untuk men-dekripsi data yang dikirimkan oleh *client* melalui *access point*.

### *D. Wi-Fi Protected Access (WPA dan WPA2)*

Menyikapi kelemahan yang dimiliki oleh WEP, telah dikembangkan sebuah teknik pengamanan baru yang disebut sebagai WPA (*Wi-Fi Protected Access*). Teknik WPA adalah model kompatibel dengan spesifikasi standar *draft* IEEE 802.11i. Teknik ini mempunyai beberapa tujuan dalam desainnya, yaitu kokoh, interoperasi, mampu digunakan untuk menggantikan WEP, dapat diimplementasikan pada pengguna rumahan atau *corporate*.

Keamanan yang ditawarkan oleh IEEE yang dikerjakan oleh *group* 802.11i akhirnya diselesaikan pada tahun 2004 dan oleh aliansi Wi-Fi level keamanan ini dinamakan sebagai WPA2. Enkripsi utama yang digunakan oleh WPA2 adalah AES (*Advanced Encryption Standard*) [2].

### *E. WPA2-RADIUS / WPA2-Enterprise*

Metode keamanan dan algoritma enkripsi pada WPA2-RADIUS ini sama saja dengan WPA *Pre-Shared Key*, tetapi autentikasinya menggunakan 802.1x atau EAP (*Extensible Authentication Protocol*).

*Setting security* WPA2-*Enterprise* ini membutuhkan sebuah *server* khusus yang berfungsi sebagai pusat auntentikasi seperti *server* RADIUS (*Remote Authentication Dial-In User Service*) . Dengan adanya RADIUS *server* ini, autentikasi akan dilakukan per-*client* sehingga tidak perlu lagi memasukkan *passphrase* atau *network key* yang sama untuk setiap *client*. "*Network key*" di sini diperoleh dan diproses oleh *server* RADIUS tersebut.

## III. PEMBAHASAN

### *A. Fase Identifikasi*

Pada tahap ini melakukan proses identifikasi terhadap jaringan *wireless* LAN dan permasalahan keamanan yang dihadapinya. Dari hasil studi pustaka didapatkan beberapa masalah keamanan sebagai berikut:

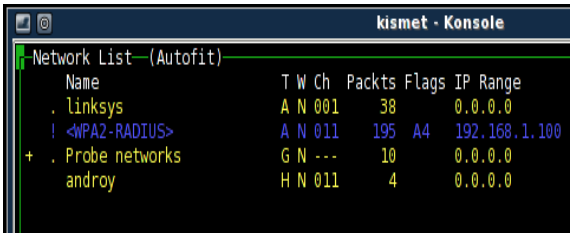
1. *Monitoring* lalu lintas jaringan.
2. Pencurian *username*, *password*, atau nomor kartu kredit.
3. Akses ilegal.
4. *Man-in-the-Middle Attacks*.

### *B. Fase Pengujian Celah Keamanan Pada WLAN*

Pada tahap ini melakukan proses pengujian terhadap beberapa jenis keamanan *wireless* LAN seperti *Hidden* SSID, MAC *Filtering*, WEP, dan WPA/WPA2. Tujuannya adalah untuk membuktikan kelemahan dari masing-masing keamanan tersebut.

#### *1) Pengujian Hidden SSID*

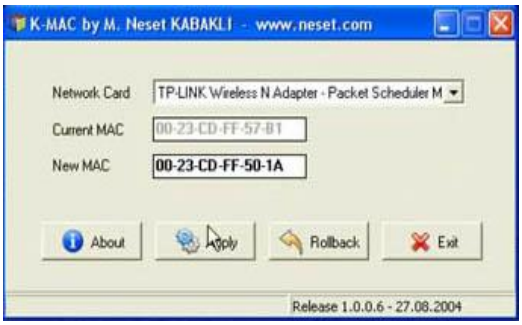
Dari hasil pengujian dengan metode passive scanning melalui aplikasi Kismet diperoleh kesimpulan bahwa SSID yang disembunyikan akan langsung terlihat.




Gambar 1. Kismet mendeteksi *Hidden* SSID

#### *2) Pengujian MAC Filtering*

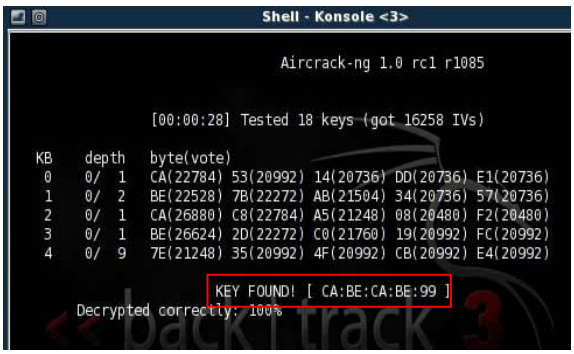
MAC *address* yang sudah ada di dalam adapter secara fisik memang benar tidak bisa diubah (kecuali mengubah *firmware*), namun secara *virtual* hal tersebut dengan mudah bisa dilakukan. Sistem operasi akan membaca informasi MAC *address* dari *hardware* adapter dan menyimpannya ke dalam file atau *registry* seperti yang dilakukan oleh Windows.




Gambar 2. Mengubah MAC *address* dengan K-MAC

#### *3) Pengujian WEP (Wired Equivalent Privacy)*

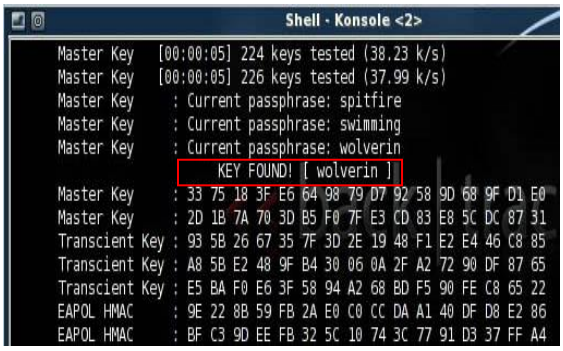
WEP *Cracking* merupakan *cracking* dengan metode statistik, karena itu untuk mendapatkan WEP *key*, dibutuhkan sejumlah data untuk dianalisa. Semakin banyak data yang terkumpul, akan semakin memudahkan proses *cracking* dalam mencari WEP *key*. Dari hasil pengujian didapatkan bahwa enkripsi yang digunakan WEP memang sangat lemah, karena dalam hitungan menit sudah berhasil dilakukan proses *cracking*.




Gambar 3. Proses *cracking* WEP

*4) Pengujian Wi-Fi Protected Access (WPA dan WPA2)*

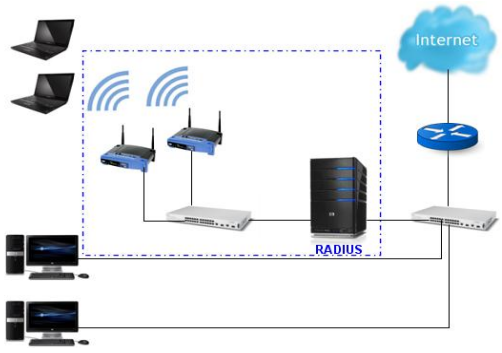
Enkripsi AES yang digunakan WPA/WPA2 sudah sangat kuat untuk saat ini. Namun akibat dari penggunaan *passphrase* yang lemah masih dimungkinkan untuk dilakukan proses *cracking* terhadap sistem keamanan ini.




Gambar 4. Proses cracking WPA/WPA2

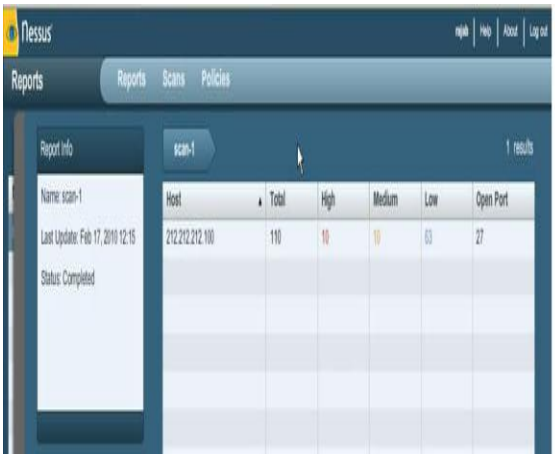
*5). Pengujian RADIUS Server*

Untuk melakukan pengujian celah keamanan pada WPA2-RADIUS kami melakukan perancangan sistem WLAN yang terhubung dengan Wired LAN, seperti pada gambar 5 dibawah ini.




Gambar 5. Topologi WPA2-RADIUS

Pengujian dilakukan untuk menemukan celah keamanan dari sistem WPA2-RADIUS. Baik melalui jaringan *wireless* LAN maupun pengujian melalui *wired* LAN. Dengan menggunakan tool nessus diperoleh data-data sebagai berikut.




Gambar 6. Pengujian RADIUS melalui *wireless* LAN

Dari pengujian diatas memperlihatkan bahwa *vulnerability* yang terdeteksi :

1. *Vulnerability* dengan resiko *high* 10 buah
2. *Vulnerability* dengan resiko *medium* 10 buah
3. *Vulnerability* dengan resiko *low* 63 buah

Setelah mengetahui *vulnerability* yang terdapat pada RADIUS *server* ini, selanjutnya dapat dilakukan proses *patch & update* untuk menutup berbagai celah berbahaya dan harus dilakukan proses *scanning* kembali untuk memastikan apakah masih terdapat *vulnerability* yang berbahayaatau tidak. . Bila masih ada, dilakukan proses *patch & update* kembali. Hal ini dilakukan beberapa kali hingga tidak ada lagi *vulnerability* yang dianggap berbahaya.

Dari hasil beberapa pengujian diatas dapat ditunjukkan bahwa masih terjadi serangan keamanan dari beberapa metode keamanan yang ada saat ini untuk jaringan WLAN. Oleh karenanya masih dieprlukan beberapa cara untuk menutupi celah keamanan tersebut.

## IV. KESIMPULAN

Kesimpulan yang didapatkan yaitu, jaringan *wireless* LAN memiliki masalah keamanan mendasar seperti *monitoring* lalu lintas jaringan, pencurian *username* & *password*, ataupun akses secara ilegal. Jenis keamanan yang biasa diterapkan seperti *Hidden* SSID, MAC *Filtering*, WEP, maupun WPA/WPA2 memiliki kelemahan masing-masing yang bisa dijebol. Begitu juga untuk WPA2-RADIUS walaupun beberapa celah kemungkinan dapat diatas dengan melakukan *patch* dan *update* namun hal ini tentu saja membuktikan bahwa metode yang ada sekarang masih rentan terhadap pembobolan keamanan. Semua bukti pembobolan kami tunjukkan pada gambar 1, gambar 2, gambar 3, gambar 4, gambar 6 dan gambar 7.

DAFTAR PUSTAKA


[1] Geier, Jim. 2005. *Wireless Networks First-Step*. Yogyakarta: Penerbit ANDI.

[2] Thomas, Tom. 2005. *Network Security First-Step*. Yogyakarta: Penerbit ANDI

[3] S'to. 2007. *Wireless Kung Fu: Networking & Hacking*. Jakarta: Jasakom

[4] Sukaridhoto, Sritrusta. 2007. *Modul Wireless*. Politeknik Elektronika Negeri Surabaya - Institut Teknologi Sepuluh Nopember (PENS-ITS). [online]. Tersedia: http://lecturer.eepis-its.edu/~dhoto/ [Akses: 17 Maret 2009, pkl. 9:15 WIB]

[5] W. Setiawan, Agung. 2005. *Remote Authentication Dial In User Service (RADIUS) untuk Autentikasi Pengguna Wireless LAN*. [makalah]. Bandung: Departemen Teknik Elektro, Fakultas Teknologi Industri, Institut Teknologi Bandung.

[6] http://id.wikipedia.org/wiki/Backtrack
[Akses: 2 Oktober 2010, pkl. 14:25 WIB ]

[7] http://en.wikipedia.org/wiki/Aircrack-ng
[Akses: 2 Oktober 2010, pkl. 14:30 WIB ]

[8] http://en.wikipedia.org/wiki/Kismet_(software)
[Akses: 2 Oktober 2010, pkl. 14:40 WIB ]