# Wireless Security (Hacking Wifi)

by
**Josua M Sinambela**
email josh at gadjahmada.edu
website http://josh.staff.ugm.ac.id

Jaringan Wifi memiliki lebih banyak kelemahan dibanding dengan jaringan kabel. Saat ini perkembangan teknologi wifi sangat signifikan sejalan dengan kebutuhan sistem informasi yang mobile. Banyak penyedia jasa wireless seperti hotspot komersil, ISP, Warnet, kampus-kampus maupun perkantoran sudah mulai memanfaatkan wifi pada jaringan masing masing, tetapi sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan wireless tersebut. Hal ini membuat para hacker menjadi tertarik untuk mengexplore keamampuannya untuk melakukan berbagai aktifitas yang biasanya ilegal menggunakan wifi.

Pada artikel ini akan dibahas berbagai jenis aktivitas dan metode yang dilakukan para hacker wireless ataupun para pemula dalam melakukan wardriving. Wardriving adalah kegiatan atau aktivitas untuk mendapatkan informasi tentang suatu jaringan wifi dan mendapatkan akses terhadap jaringan wireless tersebut. Umumnya bertujuan untuk mendapatkan koneksi internet, tetapi banyak juga yang melakukan untuk maksud-maksud tertentu mulai dari rasa keingintahuan, coba coba, research, tugas praktikum, kejahatan dan lain lain.

## Kelemahan Wireless

Kelemahan jaringan wireless secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Salah satu contoh penyebab kelemahan pada konfigurasi karena saat ini untuk membangun sebuah jaringan wireless cukup mudah. Banyak vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan wireless yang masih menggunakan konfigurasi wireless default bawaan vendor. Penulis sering menemukan wireless yang dipasang pada jaringan masih menggunakan setting default bawaan vendor seperti SSID, IP Address , remote manajemen, DHCP enable, kanal frekuensi, tanpa enkripsi bahkan user/password untuk administrasi wireless tersebut.

WEP (Wired Equivalent Privacy) yang menjadi standart keamanan wireless sebelumnya, saat ini dapat dengan mudah dipecahkan dengan berbagai tools yang tersedia gratis di internet. WPA-PSK dan LEAP yang dianggap menjadi solusi menggantikan WEP, saat ini juga sudah dapat dipecahkan dengan metode *dictionary attack* secara offline.

Beberapa kegiatan dan aktifitas yang dilakukan untuk mengamanan jaringan wireless antara lain:

1. **Menyembunyikan SSID**

Banyak administrator menyembunyikan Services Set Id (SSID) jaringan wireless mereka dengan maksud agar hanya yang mengetahui SSID yang dapat terhubung ke jaringan mereka. Hal ini tidaklah benar, karena SSID sebenarnya tidak dapat disembuyikan secara sempurna. Pada saat saat tertentu atau khususnya saat client akan terhubung (*assosiate*) atau ketika akan memutuskan diri *(deauthentication)* dari sebuah jaringan wireless, maka client akan tetap mengirimkan SSID dalam bentuk plain text (meskipun menggunakan enkripsi), sehingga jika kita bermaksud menyadapnya, dapat dengan mudah menemukan informasi tersebut. Beberapa tools yang dapat digunakan untuk mendapatkan ssid yang dihidden antara lain, kismet (kisMAC), ssid_jack (airjack), aircrack , void11 dan masih banyak lagi.

2. **Keamanan wireless hanya dengan kunci WEP**

WEP merupakan standart keamanan & enkripsi pertama yang digunakan pada wireless, WEP memiliki berbagai kelemahan antara lain :

- Masalah kunci yang lemah, algoritma RC4 yang digunakan dapat dipecahkan.
- WEP menggunakan kunci yang bersifat statis
- Masalah *initialization vector* (IV) WEP
- Masalah integritas pesan *Cyclic Redundancy Check* (CRC-32)

WEP terdiri dari dua tingkatan, yakni kunci 64 bit, dan 128 bit. Sebenarnya kunci rahasia pada kunci WEP 64 bit hanya 40 bit, sedang 24bit merupakan Inisialisasi Vektor (IV). Demikian juga pada kunci WEP 128 bit, kunci rahasia terdiri dari 104bit.

Serangan-serangan pada kelemahan WEP antara lain :

- Serangan terhadap kelemahan inisialisasi vektor (IV), sering disebut FMS attack. FMS singkatan dari nama ketiga penemu kelemahan IV yakni Fluhrer, Mantin, dan Shamir. Serangan ini dilakukan dengan cara mengumpulkan IV yang lemah sebanyak-banyaknya. Semakin banyak IV lemah yang diperoleh, semakin cepat ditemukan kunci yang digunakan

  ( www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf )

- Mendapatkan IV yang unik melalui packet data yang diperoleh untuk diolah untuk proses cracking kunci WEP dengan lebih cepat. Cara ini disebut chopping attack, pertama kali ditemukan oleh h1kari. Teknik ini hanya membutuhkan IV yang unik sehingga mengurangi kebutuhan IV yang lemah dalam melakukan cracking WEP.

- Kedua serangan diatas membutuhkan waktu dan packet yang cukup, untuk mempersingkat waktu, para hacker biasanya melakukan *traffic injection*. *Traffic Injection* yang sering dilakukan adalah dengan cara mengumpulkan packet ARP kemudian mengirimkan kembali ke access point. Hal ini mengakibatkan pengumpulan initial vektor lebih mudah dan cepat.

  Berbeda dengan serangan pertama dan kedua, untuk serangan *traffic injection,*diperlukan spesifikasi alat dan aplikasi tertentu yang mulai jarang ditemui di toko-toko, mulai dari

chipset, versi firmware, dan versi driver serta tidak jarang harus melakukan patching terhadap driver dan aplikasinya.

3. **Keamanan wireless hanya dengan kunci WPA-PSK atau WPA2-PSK**

   WPA merupakan teknologi keamanan sementara yang diciptakan untuk menggantikan kunci WEP. Ada dua jenis yakni WPA personal (WPA-PSK), dan WPA-RADIUS.

   Saat ini yang sudah dapat di crack adalah WPA-PSK, yakni dengan metode brute force attack secara offline. Brute force dengan menggunakan mencoba-coba banyak kata dari suatu kamus. Serangan ini akan berhasil jika passphrase yang yang digunakan wireless tersebut memang terapat pada kamus kata yang digunakan si hacker.

   Untuk mencegah adanya serangan terhadap keamanan wireless menggunakan WPA-PSK, gunakanlah passphrase yang cukup panjang (satu kalimat).

   Tools yang sangat terkenal digunakan melakukan serangan ini adalah CoWPAtty ( http://www.churchofwifi.org/ ) dan aircrack ( http://www.aircrack-ng.org ) . Tools ini memerlukan daftar kata atau *wordlist*, dapat di ambil dari http://wordlist.sourceforge.net/

4. **MAC Filtering**

   Hampir setiap wireless access point maupun router difasilitasi dengan keamanan MAC Filtering. Hal ini sebenarnya tidak banyak membantu dalam mengamankan komunikasi wireless, karena MAC address sangat mudah dispoofing atau bahkan dirubah.

   Tools *ifconfig* pada OS Linux/Unix atau beragam tools spt network utilitis, regedit, smac, machange pada OS windows dengan mudah digunakan untuk spoofing atau mengganti MAC address.

   Penulis masih sering menemukan wifi di perkantoran dan bahkan ISP (yang biasanya digunakan oleh warnet-warnet) yang hanya menggunakan proteksi MAC Filtering. Dengan menggunakan aplikasi wardriving seperti kismet/kisMAC atau aircrack tools, dapat diperoleh informasi MAC address tiap client yang sedang terhubung ke sebuah Access Point.

   Setelah mendapatkan informasi tersebut, kita dapat terhubung ke Access point dengan mengubah MAC sesuai dengan client tadi. Pada jaringan wireless, duplikasi MAC adress tidak mengakibatkan konflik. Hanya membutuhkan IP yang berbeda dengan client yang tadi.

5. **Captive Portal**

Infrastruktur Captive Portal awalnya didesign untuk keperluan komunitas yang memungkinkan semua orang dapat terhubung (open network). Captive portal sebenarnya merupakan mesin router atau gateway yang memproteksi atau tidak mengizinkan adanya trafik hingga user melakukan registrasi/otentikasi. Berikut cara kerja captive portal :

- user dengan wireless client diizinkan untuk terhubung wireless untuk mendapatkan IP address (DHCP)
- block semua trafik kecuali yang menuju ke captive portal (Registrasi/Otentikasi berbasis web) yang terletak pada jaringan kabel.
- *redirect* atau belokkan semua trafik web ke captive portal
- setelah user melakukan registrasi atau login, izinkan akses ke jaringan (internet)

Beberapa hal yang perlu diperhatikan, bahwa captive portal hanya melakukan tracking koneksi client berdasarkan IP dan MAC address setelah melakukan otentikasi. Hal ini membuat captive portal masih dimungkinkan digunakan tanpa otentikasi karena IP dan MAC adress dapat dispoofing. Serangan dengan melakukan spoofing IP dan MAC. Spoofing MAC adress seperti yang sudah dijelaskan pada bagian 4 diatas. Sedang untuk spoofing IP, diperlukan usaha yang lebih yakni dengan memanfaatkan ARP cache poisoning, kita dapat melakukan redirect trafik dari client yang sudah terhubung sebelumnya.

Serangan lain yang cukup mudah dilakukan adalah menggunakan Rogue AP, yaitu mensetup Access Point (biasanya menggunakan HostAP) yang menggunakan komponen informasi yang sama seperti AP target seperti SSID, BSSID hingga kanal frekwensi yang digunakan. Sehingga ketika ada client yang akan terhubung ke AP buatan kita, dapat kita membelokkan trafik ke AP sebenarnya.

Tidak jarang captive portal yang dibangun pada suatu hotspot memiliki kelemahan pada konfigurasi atau design jaringannya. Misalnya, otentikasi masih menggunakan plain text (http), managemen jaringan dapat diakses melalui wireless (berada pada satu network), dan masih banyak lagi.

Kelemahan lain dari captive portal adalah bahwa komunikasi data atau trafik ketika sudah melakukan otentikasi (terhubung jaringan) akan dikirimkan masih belum terenkripsi, sehingga dengan mudah dapat disadap oleh para hacker. Untuk itu perlu berhati-hati melakukan koneksi pada jaringan hotspot, agar mengusahakan menggunakan komunikasi protokol yang aman seperti https,pop3s, ssh, imaps dst.