

WarDriving Menggunakan Tools “Wigle” dan Mapping Menggunakan “GoogleEarth” Dikawasan PemKab OI (Ogan Ilir)

Fajri Aulia Rachmat¹(0912100101032)

¹Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Jl. Raya Palembang - Prabumulih Km 32, Kabupaten Ogan Ilir, Sumatera Selatan
E-mail: 09121001032@students.ilkom.unsri.ac.id

Abstrak

Wigle merupakan salah satu dari sekian banyak Tools yang bisa digunakan sebagai Hacking Wireless, proses yang kita lakukan saat ingin meretas atau Hacking sebuah jaringan Wireless disebut “Wardriving”. Wigle bisa digunakan pada Device sekelas smartphone, fungsinya juga tidak jauh berbeda dengan yang ada di versi PC, hanya saja ketika digunakan di smartphone fungsinya jadi jauh lebih baik karna smartphone lebih mudah dibawa ketimbang laptop. Sebagai Tools yang digunakan untuk meretas sebuah jaringan Wireless, Wigle akan sangat membantu proses Wardriving dan tentunya Wigle akan sangat berguna untuk mempelajari proteksi keamanan jaringan Wireless. Seperti yang kita ketahui, Access point yang biasa digunakan di sebuah instalasi pastinya sudah tertanam enkripsi karna Access Point tersebut menggunakan standarisasi IEEE 802.11b yang tertanam juga didalamnya WEP, WPA, WPA2. Untuk proteksi keamanan yang tinggi gunakanlah Password atau Passphrase yang unik agar keamanan yang diciptakan menjadi setingkat lebih diatas standarnya. Wigle juga bisa mengexport file dalam bentuk .kml, sehingga memudahkan kita menggunakan GoogleEarth sebagai tools pendukungnya, walaupun nantinya GoogleEarthlah yang akan digunakan untuk Mapping jaringan wirelessnya.

Kata Kunci : *Wigle, Hacking Wireless, GoogleEarth, IEEE 802.11b, Wardriving*

1. Pendahuluan

Wi-Fi, Wireless Ethernet dan Wireless LAN merupakan hal yang sangat diperlukan pada saat sekarang ini, sebab, kebutuhan setiap orang akan internet dewasa ini sangat tinggi. Oleh karena itu, sekarang banyak sekali kita lihat Access Point (AP) yang dipasang di setiap sudut ruangan ataupun ditengah tengah ruangan dengan tujuan terjangkaunya sarana internet yang lebih memadai. Wi-Fi, Wireless Ethernet dan Wireless LAN memiliki jaringan standar milik IEEE 802.11. sebagai standar yang biasa digunakan instansi yang ada Di Indonesia 802.11b adalah jaringan standar yang memiliki frekuensi 2.4GHz dengan kecepatan transfer data sebesar 11Mbps. Karna bersifat tanpa kabel (Wireless), jangkauan yang bisa di peroleh lebih jauh sehingga dapat menjangkau user yang akan menggunakan sistem ini. Keamanannya pun lebih tinggi karna teknologi ini menggunakan gelombang elektromagnetik. Namun, akibat hal ini penyebaran malware dan sering terjadinya gagal sistem sering terjadi, ini terjadi akibat dampak mobile yang secara otomatis di ciptakan sendiri oleh teknologi ini. Wardriving adalah salah satu perilaku atau kegiatan yang sekarang biasa dilakukan untuk masuk kedalam jaringan internet yang disediakan melalui Wireless Ethernet. Selain merugikan, ini akan menjadi masalah serius dikemudian hari, karna semakin banyak tools yang bisa digunakan sebagai penyokong dari Wardriving.

2. Tinjauan Pustaka

2.1 WarDriving

Wardriving adalah tindakan mencari Wi-Fi jaringan nirkabel oleh seseorang dalam kendaraan yang bergerak, menggunakan komputer portable, smartphone atau personal digital assistant (PDA). Istilah ini mulai berkembang karena teknologi yang semakin hari semakin cepat kemajuannya. Banyak programmer yang berlomba-lomba membuat tools baru untuk membobol jaringan yang bersifat Wireless.

2.2 Wigle

Wigle adalah salah satu dari sekian banyak tools yang digunakan untuk menjalankan maksud dari Wardriving yaitu untuk Hacking Wireless. Wigle berbasis android walaupun wigle sendiri juga tersedia dalam versi PC, namun smartphone berbasis android lebih mudah dibawa daripada menggunakan laptop atau notebook, itulah mengapa Wigle lebih mudah digunakan pada smartphone. NetStumbler juga merupakan salah satu tools yang bisa digunakan untuk Wardriving, kelemahan dari NetStumbler adalah kita perlu menambah Hardware yaitu GPS yang bisa dihubungkan menggunakan kabel connector Db9 yang ada dibelakan CPU PC, namun tentu saja itu akan memakan biaya lebih untuk pengaplikasiannya.

2.3 Wireless Access Point

Wireless Access Point (WAP) dalam jaringan komputer, titik akses nirkabel adalah suatu peranti yang memungkinkan peranti nirkabel untuk terhubung ke dalam jaringan dengan menggunakan Wi-Fi, Bluetooth, atau standar lain. WAP biasanya tersambung ke suatu *router* (melalui kabel) sehingga dapat meneruskan data antara berbagai peranti nirkabel (seperti komputer atau pencetak) dengan jaringan berkabel pada suatu jaringan. Standar yang diterapkan untuk WAP ditetapkan oleh IEEE dan sebagian besar menggunakan IEEE 802.11. WAP terhubung pada jaringan, pada jarak jangkauan WAP siapapun dapat terhubung ke jaringan. Pada saat ini enkripsi merupakan keamanan standar yang harus dimiliki oleh setiap Access Point yang digunakan sebagai sistem keamanan yang akan menjamin keamanan user. Generasi enkripsi pertama yang diterapkan adalah Wired Equivalent Privacy (WEP), WEP sendiri telah banyak diuji karena memiliki banyak kelemahan sehingga sangat mudah untuk ditembus. Generasi kedua dan ketiga adalah menggunakan Wi-Fi Protected Access (WPA), Beberapa WAP mendukung authentication menggunakan Remote Authentication Dial-In User Service (RADIUS) dan server authentication yang lain. dan digenerasi yang sama Wi-Fi Protected Access II (WPA2), keduanya memiliki algoritma yang kuat dan aman jika menggunakan password atau passphrase yang kuat (unik).

2.4 Global Position System

Global Position System (GPS) adalah sistem untuk menentukan letak di permukaan bumi dengan bantuan penyelarasan (*synchronization*) sinyal satelit. Sistem ini menggunakan 24 satelit yang mengirimkan sinyal gelombang mikro ke Bumi. Sinyal ini diterima oleh alat penerima di permukaan, dan digunakan untuk menentukan letak, kecepatan, arah, dan waktu. Sistem yang serupa dengan GPS antara lain GLONASS Rusia, Galileo Uni Eropa, IRNSS India.

2.5 Google Earth

Google Earth merupakan sebuah program globe virtual yang sebenarnya disebut Earth Viewer dan dibuat oleh Keyhole, Inc.. Program ini memetakan bumi dari superimposisi gambar yang dikumpulkan dari pemetaan satelit, fotografi udara dan globe GIS 3D.

3. Metode Penelitian

Pada penelitian kali ini, saya selaku penulis menggunakan android milik teman saya sebagai device yang saya gunakan. Kami menginstal Wigle sebagai aplikasi atau Tools yang bisa digunakan untuk Wardriving. Kami berangkat menggunakan motor, Kami melaju lambat ke kawasan PemKab OI (Ogan Ilir), setibanya disana kami langsung melakukan scanning. teman saya bertugas sebagai pemegang device, karna saat melakukan wardriving SSID yang telah didapat haruslah disimpan atau di export ke format KML dengan cepat agar SSID yang sudah di dapat tidak hilang ketika akan disimpan.

4. Hasil Penelitian dan Analisa

4.1 Hasil



Gambar 1



Gambar 2

4.2 Analisa

Setelah melakukan scanning di kawasan PemKab OI (Ogan Ilir) didapatkan file format .kml yang kami export dari Wigle, dan kami langsung membuka file tersebut dengan menggunakan GoogleEarth, hasil yang didapat dari GoogleEarth adalah mapping yang bisa dilihat pada Gambar 1, dapat dilihat pada mapping bahwasannya hasil scanning juga mengenai beberapa Access Point milik beberapa Provider terkenal yang ada Di Indonesia yang juga memiliki Hotspot dikawasan tersebut. Hasil pada Gambar 1 merupakan hasil yang kami dapat setelah beberapa kali mengitari kawasan PemKab OI (Ogan Ilir). Pada gambar 1 terlihat ada ikon berwarna merah dan hijau, ikon berwarna merah menyatakan bahwa Access Point (AP) tersebut dilindungi oleh password dengan metode autentikasi WEP/WPA PSK/WPA2-PSK, sementara ikon yang berwarna hijau menyatakan bahwa Access Point (AP) tersebut menggunakan metode autentikasi dengan servis RADIUS.

Lalu, pada Gambar 2, terlihat kotak putih yang bertuliskan Pemkab-OI@wifi.id yang merupakan sebuah Access Point dengan SSID tersebut. Lokasi Access Point ini sendiri tersebar di beberapa titik karena banyak sekali SSID serupa yang kami temukan. (Gambar 1). Access Point (AP) ini didukung oleh keamanan enkripsi WPA atau WPA2, dari Gambar 2 juga didapatkan BSSID 6c:99:89:8a:c3:d2. Paket bound untuk perangkat dalam WLAN harus menuju ke tempat yang benar, SSID menjaga paket dalam WLAN yang benar, bahkan walaupun adanya tumpang tindih WLAN. Namun, biasanya ada beberapa jalur akses dalam setiap WLAN, dan harus ada cara untuk mengidentifikasi titik-titik akses dan klien terkait. Pengenal ini disebut basic service set identifier (BSSID) dan termasuk dalam semua paket nirkabel.

5. Kesimpulan

Dalam perkembangannya , keamanan jaringan wireless haruslah menjadi sesuatu yang diperhatikan, sebab , bahkan dengan menggunakan tools sederhana seperti Wigle dan netstumbler saja , kamanan yang ada pada sebuah jaringan wireless akan sangat riskan semakin banyak upaya dari seorang hacker untuk membobol ataupun meretas sebuah jaringan wireless. Dalam penelitian kali ini didapatlah kesimpulan yang tentunya berdasarkan apa yang terjadi dilapangan.

1. Wigle sebagai Tools yang digunakan pada smartprhone bisa menggantikan fungsi wi-fi searching yang ada pada smartphone tersebut, namun perbedaannya adalah pada saat penggunaannya , wi-fi searching pada smartphone digunakan untuk menghubungkan smartphone ke Access Point (AP) yang ada disekitar smartphone tersebut , sementara Wigle difungsikan untuk mengetahui ada atau tidaknya Access Point (AP) di sekitar smartphone tersebut.
2. Pada penelitian kali ini , dapat diketahui bahwasannya GoogleEarth bisa digunakan untuk mapping sebuah jaringan wireless sebagai pendukung kegiatan Wardriving, dan juga dapat mengetahui SSID serta BSSID yang ada pada jaringan wireless tersebut ,tentu saja mapping bisa dilakukan dengan format file .kml yang diberikan oleh Wigle.

6. Daftar Pustaka

- <https://en.wikipedia.org/wiki/Wardriving> (28-04-2016)
- https://en.wikipedia.org/wiki/Wireless_access_point (28-04-2016)
- https://id.wikipedia.org/wiki/Google_Earth (28-04-2016)
- <http://www.datasurvey.com/artikel/pengertian-gps-global-positioning-system>. (29-04-2016)
- https://id.wikipedia.org/wiki/Sistem_Pemosisi_Global (29-04-2016)
- http://www.juniper.net/documentation/en_US/network-director1.5/topics/concept/wireless-ssid-bssid-ssid.html (29-04-2016)