TUGAS KEAMANAN JARINGAN KOMPUTER
WARDRIVING MENGGUNAKAN APLIKASI WIGLE

Disusun Oleh:

Nama : MUHAMMAD FAJAR PUTRA
NIM : 09011181520009
Kelas : SK8

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2019

WARDRIVING MENGGUNAKAN APLIKASI “WIGLE”

Muhammad Fajar Putra

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Jl. Raya Palembang - Prabumulih Km 32, Kabupaten Ogan Ilir, Sumatera Selatan

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 ,fungsiya 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 kemanan 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 GooglEarth sebagai tools pendukungnya,walaupun nantinya GoogleEarthlah yang akan digunakan untuk Mapping jaringan wirelessnya.

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 karna 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 memliki 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 karna 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 berbasi android lebih mudah dibawa dari pada menggunaka 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 kaan menjamin keamanan user. Generasi enkrispi pertama yang diterapkan adalah Wired Equivalent Privacy (WEP), WEP sendiri telah banyak diuji karna memeliki banyak kelemaha 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.

3. Alat dan Langkah Langkah

Alat yang digunakan dalam wardriving ini adalah :

1. Smartphone
2. Aplikasi WiGLE wifi

Langkah Langkah

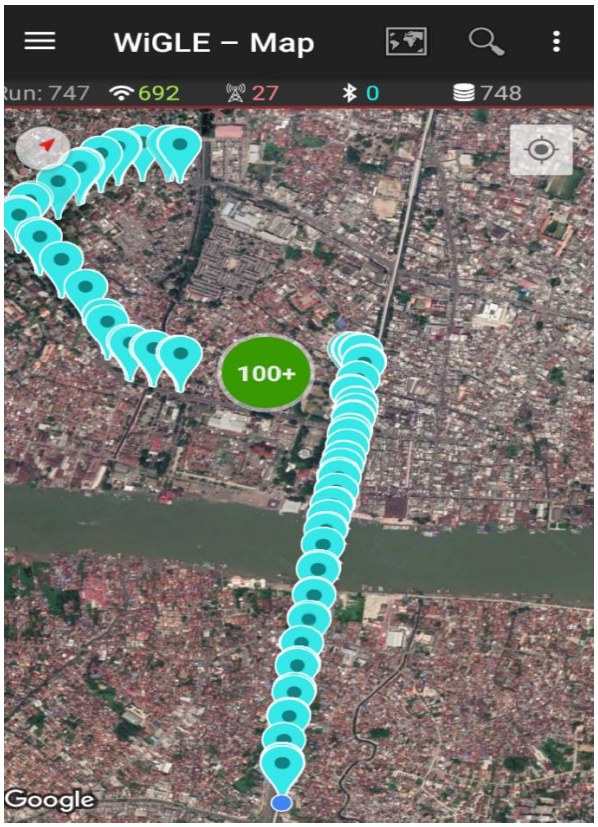
1. Hidupkan Wifi dan GPS
2. Masuk WiGLE wifi dan hidupkan scan
3. Jalan sampai ke tujuan

4. Tujuan

Tujuan dari wardriving adalah mengindari serangan serangan seperti dibawah ini :

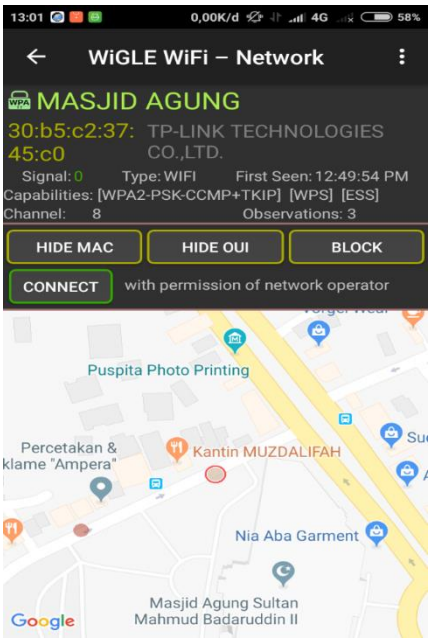
1. MAC Address Spoofing
   merupakan varian dari logical attack dalam wireless penetration testing. Dimana attacker berusaha menyembunyikan mac address sesungguhnya dengan menjiplak mac address dari salah satu user yang valid dalam suatu network sehingga attacker dapat melakukan koneksi dan dianggap oleh mesin sebagai user yang berhak melakukan akses.
2. Serangan Denial of Service
   Denial of Service adalah kegiatan membanjiri packet dalam suatu jaringan sehingga terjadi request time out. Pada jaringan wireless yang berprinsip broadcast serangan ini lebih mudah di implemantasikan.
3. Serangan Man in the Middle
   Sebuah aksi sniffing yang memanfaatkan kelemahan switch dan kesalahan penangannan ARP chache dan TCP/IP. Ide awalnya adalah menempatkan komputer attacker ditengah dua komputer yang sedang berhubungan sehingga paket data harus melalui komputer attacker terlebih dahulu agar paket data dapat dilakukan sniffing (pengintipan paket).

5. Hasil Penelitian dan Analisa



Gambar 1.

Gambar 1 adalah hasil wardriving yang telah saya lakukan menggunakan aplikasi WiGle. Rute yang saya lalui yaitu dari jalan Radial, kemudian melalui jalan Merdeka hingga melewati jembatan Ampera.



Gambar 2.

Gambar 2 adalah salah satu contoh akses point yang saya dapatkan pada saat melakukan wardriving.Nama akses point tersebut yaitu Masjid Agung Access Point (AP) ini didukung oleh keamanan enkripsi atau WPA2-PSK, dari Gambar 2 juga didapatkan BSSID 30:b5:c2:37:45:c0. 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. Kita juga dapat mengetahui seberapa kuat sinyal wifi, dan vendor dari wifi tersebut.

6. Kesimpulan

Dalam perkembangannya , keamanan jaringan wireless haruslah menjadi sesuatu yang diperhatikan, sebab , bahkan dengan menggunakan tools sederhana seperti wigle dan netstumbler saja , kemanan 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. Semakin luas daerah yang menjadi target untuk proses wardriving, maka semakin banyak potensial ditemukan access point yang menjadi sumber wi-fi.
2. Jarak menentukan kuat lemahnya sinyal access point, semakin jauh pengguna dari jangkauan access point maka semakin lemah sinyal.
3. Access point yang memiliki proteksi pada jaringannnya, misalnya access point yang dilindungi oleh password SSID(WPA2 – PSK atau WPA PSK) masih rentan (vulnerable) dari ancaman dari pihak asing (attacker) dari ancaman attacker, apalagi access point yang tidak memiliki sistem proteksi pada jaringannya sama sekali.

7. Daftar Pustaka

- *https://en.wikipedia.org/wiki/Wardriving*
- *https://en.wikipedia.org/wiki/wireless_access_point*
- *https://id.wikipedia.org/wiki/Sistem_Pemosisi_Global*
- *http://www.juniper.net/documentation/en_US/networkdirector1.5/topics/concept/wireless-ssid-bssid-essid.html*