Keamanan Jaringan Komputer

(War Driving Dikawasan Universitas Sriwijaya Indralaya)

Nama : M.Kadapi

Nim : 09011181520119

Dosen Pengampuh : Deris Setiawan.M.T,Phd

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2019

1. Pendahuluan

Jaringan 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 memliki frekuensi 2.4GHz dengan kecepatan transfer data sebesar 11Mbps. Karna bersifat nirkabel (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 ialah suatu kegiatan mencari keberadaan jaringan Wireless LAN (802.11) dan menandai lokasi akses point yang ditemukan, sambil berkendara di suatu daerah tertentu (biasanya dalam suatu kota). Biasanya yang menjadi incaran wardriver ialah jaringan nirkabel yang tidak diberi password atau enkripsi untuk melindunginya. Kegiatan ini bukan pekerjaan yang sulit dan membutuhkan peralatan yang rumit. Wardriving dapat dilakukan hanya dengan menggunakan laptop atau PDA (Personal Digital Assistant) yang dilengkapi dengan perangkat lunak yang tersedia secara gratis di internet. Perangkat tambahan yang dibutuhkan pun mudah diperoleh seperti antenna, wireless card untuk menghubungkan ke antenna serta perangkat GPS. Langkah-langkah yang harus dilakukan pun banyak tersedia di internet. Tidak perlu kesulitan mencari tutorial melakukan wardriving.

2.2 Wigle Wi-Fi

Gambar 2.2 Wigle Wi-Fi

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 Global Positioning System

Global Positioning System (GPS) adalah sistem navigasi yang dapat menentukan posisi sasaran dengan ketepatan tinggi dalam waktu yang singkat (Widodo, 2009). GPS bekerja pada referensi waktu yang sangat teliti dan memancarkan data yang menunjukkan lokasi dan waktu pada saat itu (Puntodewo dkk., 2003). Operasi dari seluruh satelit GPS yang ada disinkronisasi sehingga memancarkan sinyal yang sama. Alat penerima GPS akan bekerja jika ia menerima sinyal dari sedikitnya 4 buah satelit GPS, sehingga posisinya dalam tiga dimensi bisa dihitung. Pada saat ini, sedikitnya ada 24 satelit GPS yang beroperasi setiap waktu dan dilengkapi dengan beberapa cadangan. Satelit tersebut mengorbit selama 12 jam (dua orbit per hari) pada ketinggian sekitar 11.500 mil dan bergerak dengan kecepatan 2000 mil per jam (Puntodewo dkk., 2003). Sejak pemanfaatan NAVSTAR GPS (Navigation Satellite Timing and Ranging Global Positioning System) untuk

kepentingan sipil diperbolehkan oleh Pemerintah Amerika Serikat pada tahun 1983, maka optimalisasi penggunaan GPS untuk berbagai aplikasi semakin luas (Abidin, 2000; Ekawati, 2010).

2.4 Google Earth

Gambar 2.4 Google Earth

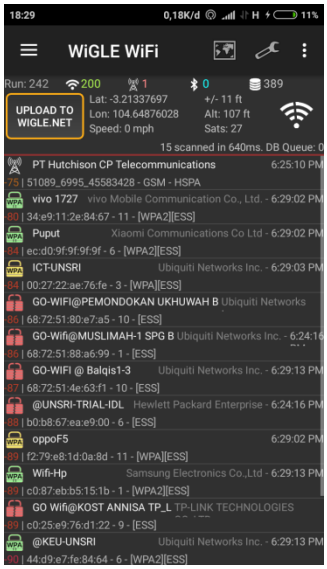
Menurut Yeyep Yousman (2008:3) *google earth* adalah aplikasi pemetaan interaktif yang di keluarkan *Google* yang dapat menampilkan peta bola dunia, keadaan topografi, foto satelit, *terrain* dapat di *overlay* dengan jalan, bangunan, lokasi ataupun informasi geografis lainnya. Sedangkan menurut Sutanto dalam Kreatif Geografi (2008: 50), *Google earth* merupakan program pemetaan bumi dari superimposisi gambar yang dikumpulkan dari pemetaan satelit, fotografi udara dan globe GIS 3D.

3. Metode Penelitian

Pada percobaan kali ini, daerah yang akan dijelajahi adalah kampus Universitas Sriwijaya Indralaya. Tindakan wardriving menggunakan kendaraan sepeda motor untuk menjelajahi targer, dengan kecepatan lebih kurang 30KM/Jam, setelah itu mulai menghidupkan GPS pada smartphone android dan membuka aplikasi WiGle wifi. Dalam perjalanan menuju ke daerah tersebut, aplikasi pada smartphone telah mulai melakukan scanning wireless network, scanning sendiri tidak memerlukan seluler data karena hanya membutuhkan GPS sebagai pemberitahu lokasi, kemudian setelah beberapa saat sudah terlihat kumpulan wireless network muncul pada layar smartphone, kemudian setelah mendapatkan kumpulan wireless network yang diinginkan, maka database diekport dalam bentuk file dengan format.kml dimana file ini akan diimport kedalam google earth untuk mendapatkan hasil mapping berupa lokasi wireless network yang ada pada daerah tersebut.

4. Hasil Penelitian

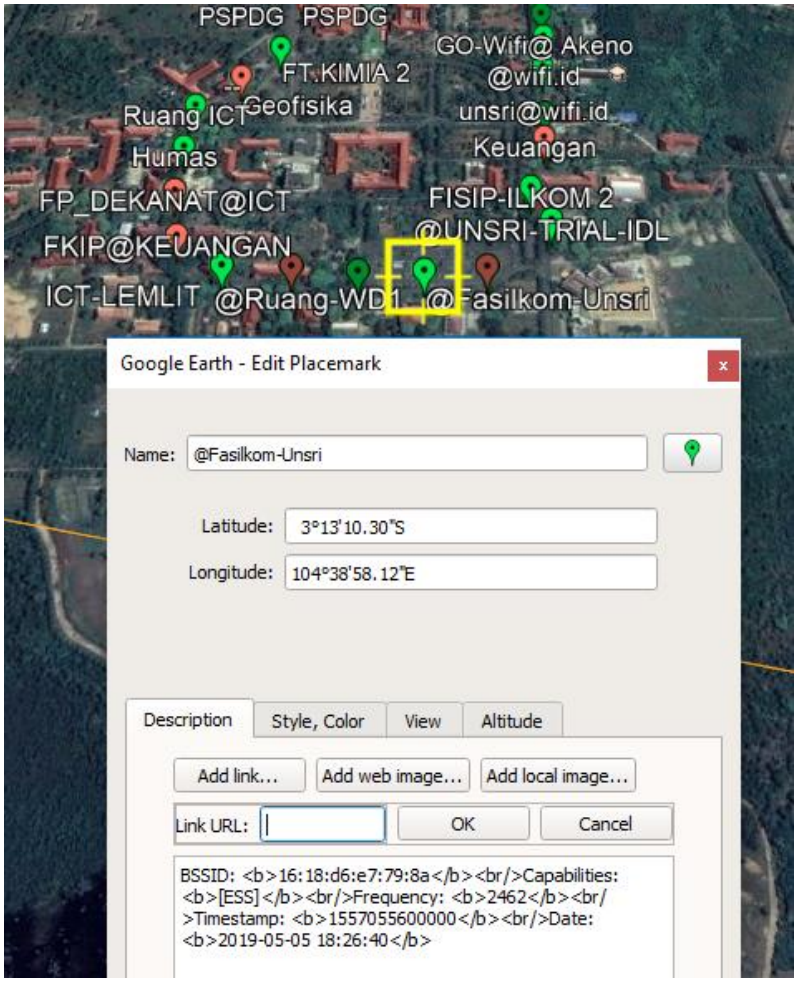
4.1. Hasil dari proses scanning wireless network dengan menggunakan aplikasi Wigle Earth adalah sebagai berikut :



Gambar 4.1. hasil scanning menggunakan Wigle Wi-Fi

4.2. Hasil dari proses mapping wireless network dengan menggunakan aplikasi Google Earth adalah sebagai berikut :

Gambar 4.2. hasil mapping menggunakan Google Earth.



Gambar 4.3. access point @Fasilkom-Unsri

5. Analisa

Setelah melakukan scanning dengan menggunakan Wigle Wi-Fi di kawasan Universitas Sriwijaya Indralaya kami mendapatkan network wireless yang kemudian kami export dengan format.kml pada Gambar 4.1, kemudian akan diimport dengan menggunakan GoogleEarth, setelah diimport akan mendapatkan hasil dari GoogleEarth yaitu mapping yang bisa dilihat pada Gambar 4.2, 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. Pada gambar 4.2 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 4.3 @Fasilkom-Unsri merupakan sebuah Access Point dengan SSID tersebut. lokasi Access Point ini sendiri berada di Fasilkom. Access Point (AP) ini

didukung oleh keamanan enkripsi WPA atau WPA2, dari Gambar 4.3 juga didapatkan BSSID 16:18:d6:e7:79:8a, capabilitas [ESS], frequensi 2462, timestamp 1557055600000, waktu 2019-05-05 18:26:40. 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.

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. Wigle Wi-Fi salah satu Tools yang digunakan untuk menscanning yang fungsinya untuk mengetahui ada atau tidaknya Access Point (AP) di sekitar smartphone tersebut.

2. Google Earth bisa digunakan untuk mapping sebuah jaringan wireless sebagai pendukung kegiatan Wardriving, dan juga dapat mengetahui SSID serta BSSID yang ada pada jaringan wireless tersebut, mapping bisa dilakukan dengan format file.kml yang diexport dari Wigle kemudian diimport dengan menggunakam Google Earth.