KEAMANAN JARINGAN KOMPUTER

"WARDRIVING"

OLEH:

Doni Saputra (09011181520120)

Dosen Pengampuh : DERIS STIAWAN, M.T., PH.D.

Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2019

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. 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 maslah 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 berbasis 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 system 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 dipermukaan 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

Percobaan yang dilakukan dari UNSRI - KM. 32 TIMBANGAN dengan cara:

a. Scanning dengan tools Wigle.
b. Import file KML menggunakan Google Earth.
c. Import file CSV menggunakan Microsoft Excel.

4. Hasil dan Analisa

Dari percobaan yang dilakukan didapat:

4.1. Hasil

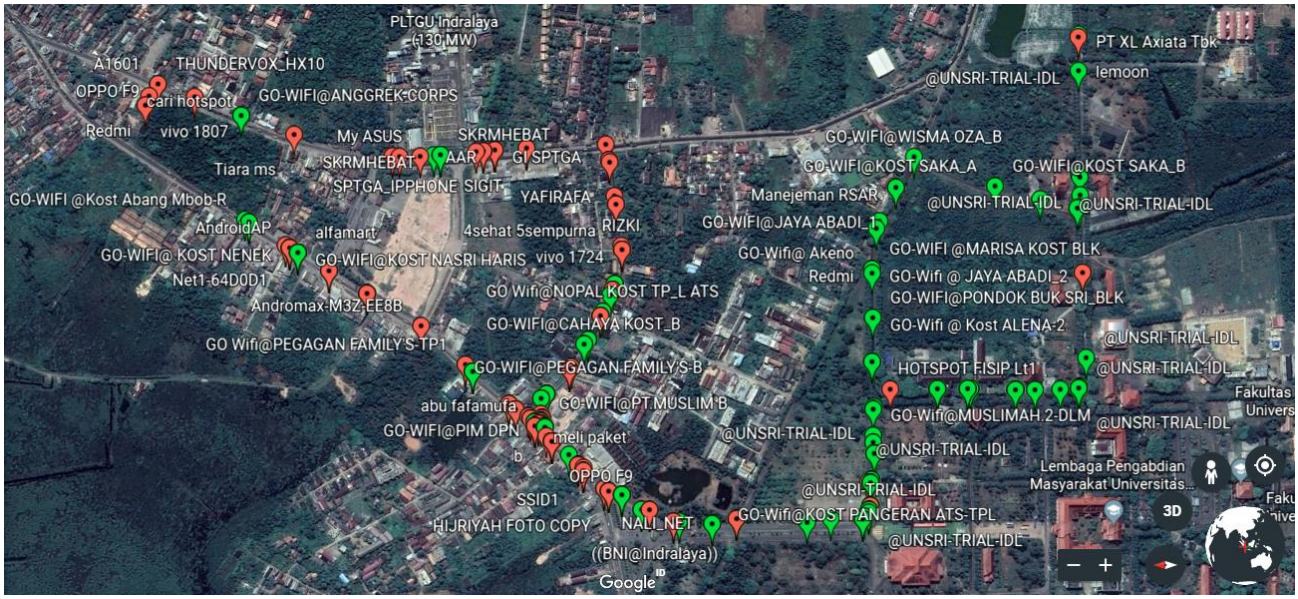
a. Hasil dari scanning didapat berupa file WigleWifi_20190505205603.kml dan WigleWifi_20190505205559.csv

b. Hasil dari Import file.csv yaitu beberapa informasi penting dari WIFI atau jaringan nirkabel yang terdeteksi diantaranya yaitu MAC, SSID, dan Mode Autentikasi.

MAC Address	SSID	AuthMode
38:17:c3:e8:c4:80	@UNSRI-TRIAL-IDL	[ESS]
74:da:38:3e:81:98	MUSIRAWAS-2	[ESS]
38:17:c3:e7:97:40	@UNSRI-TRIAL-IDL	[ESS]
00:02:6f:24:1b:72	MUSIRAWAS-1	[ESS]
a8:9f:ba:5e:de:71	tm13	[WPA2-PSK-CCMP][ESS]
b0:b8:67:ea:9f:20	@UNSRI-TRIAL-IDL	[ESS]
51011_27007_70586629	PT XL Axiata Tbk	LTE;id
51011_27007_70586629	PT XL Axiata Tbk	LTE;id

Tabel 1. Informasi WIFI

c. Hasil pemetaan menggunakan google earth.



Gambar 1. Mapping

4.2.Analisa

Pada tabel terlihat bahwa beberapa informasi penting dari WIFI atau jaringan nirkabel yang terdeteksi diantaranya yaitu MAC, SSID, dan Mode Autentikasi.

WIFI dengan SSID: **@UNSRI-TRIAL-IDL** tersebut bersifat non secured atau tidak dilindungi oleh metode autentikasi WEP/WPA PSK/WPA2-PSK. Namun, untuk WIFI dengan SSID: **tm13** bersifat secured atau dilindungi dengan metode autentikasi [WPA2-PSK-CCMP].

WIFI yang tidak memiliki metode autentikasi berpeluang besar dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan tindakan cyber crime pada jaringan tersebut.

5. Kesimpulan

1. Wigle sebagai Tools yang digunakan pada smartprhone bisa menggantikan fungsi wifi searching yang ada pada smartphone tersebut, namun perbedaannya adalah pada saat penggunannya, 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. Informasi yang didapat berupa titik akses wifi yang didapat oleh wiggle lalu dipetakan dengan google earth dan Mac address, SSID, dan mode autentikasi dari WIFI yang terdeteksi oleh wiggle.

DAFTAR PUSTAKA

- https://en.wikipedia.org/wiki/Wardriving.
- https://en.wikipedia.org/wiki/Wireless_access_point.
- https://id.wikipedia.org/wiki/Google_Earth.
- http://www.dutasurvey.com/artikel/pengertian-gps-global-positioning-system
- https://id.wikipedia.org/wiki/Sistem_Pemosisi_Global.
- http://www.juniper.net/documentation/en_US/networkdirector1.5/topics/concept/wireless-ssid-bssid-essid.html