LAPORAN KOMUNIKASI DATA
TRACKING SSID MENGGUNAKAN WIGLE WIFI

Disusun Oleh :

Sri Retno Rahayu

(09011381621069)

Dosen Pengampuh :

Deris Stiawan, M.T, Ph.D.

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

DAFTAR ISI

BAB I
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 maslah serius dikemudian hari , karna semakin banyak tools yang bisa digunakan sebagai penyokong dari Wardriving.

BAB II
Tinjauan Pustaka

A. 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.

B. 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.

C. 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).

D. ESS (Extended service set)

Extended Service Sets (ESSs) adalah kumpulan dari beberapa topologi BSS. Pada topologi ESS terdapat lebih dari satu Access Point(AP), Access Point – Access Point dalam topologi ESS terhubung satu sama lain melalui port uplink. Alasan utama dipakainnya model topologi ini adalah untuk memperluas daya jangkau AP dan juga karena meningkatnya beban yang mesti dilayani oleh satu AP.

Beberapa hal yang mesti diperhatikan adalah dalam sebuah topologi ESS, AP-AP yang ada harus beroperasi dengan channel yang berbeda agar tidak saling menginterferensi dan harus tetap menggunakan SSID yang sama.

E. WEP (Wired equivalent privacy)

WEP merupakan standart keamanan & enkripsi pertama yang digunakan pada wireless, WEP (Wired Equivalent Privacy) adalah suatu metode pengamanan jaringan nirkabel,atau disebut juga dengan Shared Key Authentication. Shared Key Authentication adalah metoda otentikasi yang membutuhkan penggunaan WEP. Enkripsi WEP menggunakan kunci yang dimasukkan (oleh administrator) ke client maupun access point. Kunci ini harus cocok dari yang diberikan akses point ke client, dengan yang dimasukkan client untuk authentikasi menuju access point, dan WEP mempunyai standar 802.11b.

Proses Shared Key Authentication: 1. Client meminta asosiasi ke access point, langkah ini sama seperti Open System Authentication. 2. Access point mengirimkan text challenge ke client secara transparan. 3. Client akan memberikan respon dengan mengenkripsi text challenge dengan menggunakan kunci WEP dan mengirimkakembali ke access point. 4. Access point memberi respon atas tanggapan client, akses point akan melakukan decrypt terhadap respon enkripsi dari client untuk melakukan verifikasi bahwa text challenge dienkripsi dengan menggunakan WEP key yang sesuai. Pada proses ini, access point akan menentukan apakah client sudah memberikan kunci WEP

yang sesuai. Apabila kunci WEP yang diberikan oleh client sudah benar, maka access point akan merespon positif dan langsung meng-authentikasi client. Namun bila kunci WEP yang dimasukkan client adalah salah, maka access point akan merespon negatif dan client tidak akan diberi authentikasi. Dengan demikian, client tidak akan terauthentikasi dan tidak tersambung dengan jaringan.

Kelebihan WEP

User lebih mudah menggunakan tipe kemanan jaringan ini karena akan secara otomatis masuk ke jaringan dengan hanya memasukan Username dan Password.

Kelemahan WEP. Masalah kata sandi yang lemah, algoritma RC4 yang digunakan dapat di bobol. karena WEP menggunakan kunci yang bersifat statis.

F. WPA (Wi-fi Protect access)

WPA merupakan salah satu tipe keamanan jaringan nirkabel yang merupakan perkembangan dari WEP, WPA secara resmi di perkenalkan pada tahun 2003, setahun sebelum WEP resmi tidak di gunakan lagi. konfigurasi WPA yang paling umum adalah WPA-PSK (Pre-Shared Key). Enkripsi yang di gunakan oleh WPA adalah 256-bit, WPA mengimplementasikan layer IEEE yaitu Layer 802.11i . WPA di desain untuk menggantikan metode keamanan WEP, yang menggunakan kunci keamanan static, WPA menggunakan metode TKIP (Temporal Key Integrity Protocol) yang mampu berubah secara dinamis. Protokol TKIP akan mengambil kunci utama sebagai starting point yang kemudian secara reguler berubah sehingga tidak ada kunci enkripsi yang digunakan dua kali. WPA juga menggunakan alat tambahan yaitu PC, Alasannya karena PC berguna sebagai authentication server yang akan memberikan kunci berbeda pada masing - masing user.

Kelebihan WPA

Enkripsi data yang digunakan adalah Temporal Key Integrity Protocol (TKIP). enkripsi yang digunakan masih sama dengan WEP yaitu RC4, karena pada dasarnya WPA ini merupakan perbaikan dari WEP dan bukan suatu level keamanan yang benar – benar baru, walaupun beberapa device ada yang sudah mendukung enkripsi AES yaitu enkripsi dengan keamanan yang paling tinggi.

Kelemahan WPA

Kelemahan WPA sampai saat ini adalah proses kalkulasi data yang lama. Dengan kata lain, proses transmisi data akan menjadi lebih lambat di bandingkan jika kita menggunakan protokol WEP tetapi Belum semua wireless mendukung, biasanya butuh upgrade firmware, driver atau bahkan menggunakan software tertentu.

G. WPA2 (Wi-fi protect access 2)

WPA telah dikembangkan pada 2006 dan secara resmi digantikan oleh WPA2. Salah satu perubahan yang paling signifikan antara WPA dan WPA2 adalah penggunaan algoritma AES dan pengenalan CCMP (Counter Cipher Mode dengan Blok Chaining Message Authentication Code Protocol) sebagai pengganti TKIP. perlu di ketahui bahwa algoritma AES merupakan Enkripsi yang memiliki keamanan paling tinggi. WPA sendiri di bagi menjadi dua jenis yaitu WPA2 Enterprise dan WPA2 Personal.

H. WPS (Wi-Fi protected setup)

WPS adalah standar jaringan nirkabel yang mencoba untuk membuat koneksi antara router dan perangkat nirkabel lebih cepat dan lebih mudah. Ia bekerja hanya untuk jaringan nirkabel yang memiliki keamanan (secutiry) WPA Personal atau WPA2 Personal. WPS tidak memberikan dukungan untuk jaringan nirkabel menggunakan keamanan WEP lawas. Dalam pengaturan normal, kamu tidak bisa menghubungkan perangkat nirkabel ke jaringan nirkabel kecuali kamu mengetahui nama jaringan (biasa disebut SSID) dan password (juga sering disebut key WPA-PSK). Pada perangkatmu, kamu harus terlebih dulu memilih jaringan yang ingin dihubungkan dan kemudian memasukkan password keamanan. Di sinilah fungsi WPS, yaitu menyederhanakan proses koneksi.

I. 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.

J. 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.

K. SSID

SSID (Service Set Identifier) merupakan identifikasi atau nama untuk jaringan Wireless. Setiap peralatan Wi-Fi harus menggunakan SSID (Service Set Identifier) tertentu. Peralatan Wi-Fi dianggap satu jaringan jika menggunakan SSID (Service Set Identifier) yang sama. Agar dapat berkomunikasi, setiap peralatan Wireless haruslah menggunakan SSID (Service Set Identifier) bersipat case-sensitive, penulisan huruf besar dan huruf kecil akan sangat berpengaruh.

SSID adalah sebuah metode/ cara jaringan wireless yang digunakan sebagai pengenal atau nama sebuah WLAN. Singkatnya dalam bahasa inggris "Public name of wireless network service". Kepanjangan dari SSID itu sendiri adalah Service Set IDentifier. SSID ini pula merupakan sebuah token yang bisa mengenal jaringan wireless dengan standar perangkat bernomor 802.11. SSID mempunyai 32 karakter khusus yangmenampilkan identifier sebagai header paket yang dikirim melalui WLAN. Identifier ini bertugas sebagai password level device ketika perangkat mobile yang mencoba untuk connect ke Basic Service Set (BSS).

Pada SSID, semua access point dan semua device berusaha untuk connect ke WLAN, dan WLAN tersebut harus mempunyai SSID yang sama. Sebuah device tidak diizinkan untuk bergabung pada BSS kecuali device tersebut menyediakan SSID khusus. Karena sebuah SSID dapat mengenali suatu teks sederhana dalam sebuah paket, dan tidak menyediakan keamanan untuk sebuah jaringan. Kadang-kadang SSID berhubungan dengan jaringan sebagai nama jaringan. SSID dalam jaringan computer client dapat juga menset access point secara manual.

Dalam penjelesan diatas bisa ditarik kesimpulan bahwa SSID tersebut merupakan tempat untuk mengisikan nama dari access point yang akan disetting. Apabila klien komputer sedang mengakses kita misalnya dengan menggunakan super scan, maka nama yang akan timbul adalah nama SSID yang diisikan tersebut.

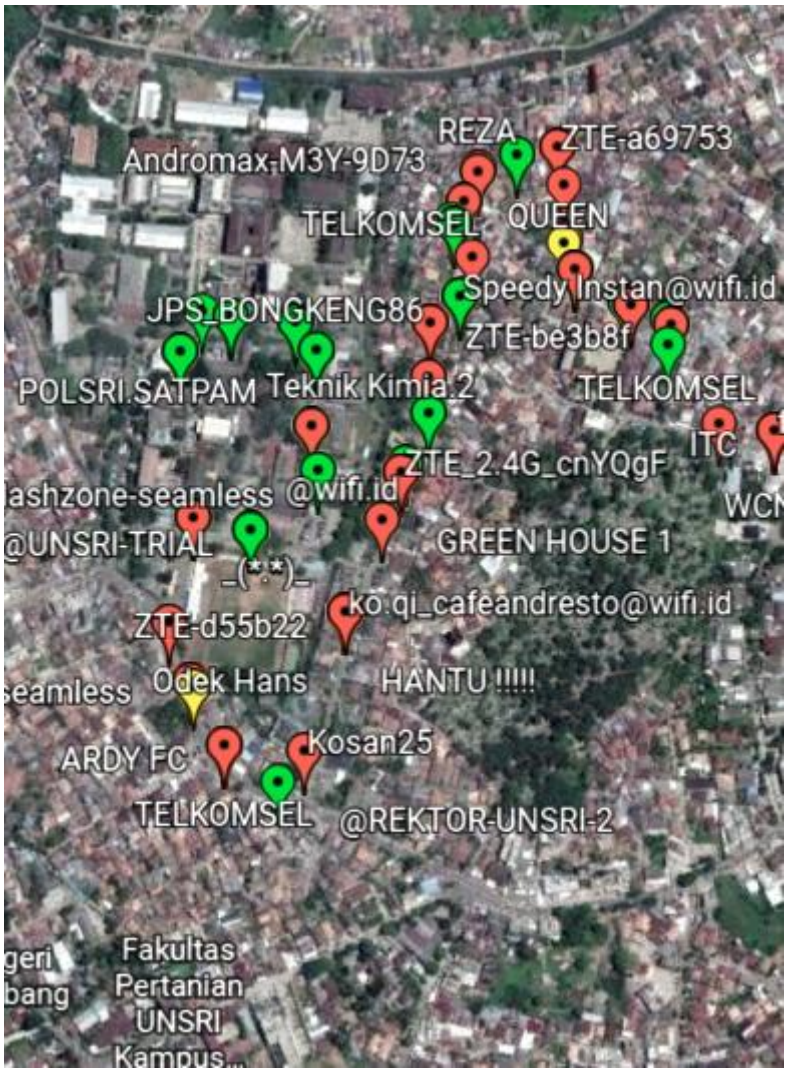
BAB III
Metode Pengamatan

Pada penelitian kali ini , saya menggunakan android sebagai device yang saya gunakan. Saya menginstal Wigle sebagai aplikasi atau Tools yang bisa digunakan untuk Wardriving. Dalam aplikasi Wigle wifi ini akan di tracking semua SSID yang berada dalam jangkauan sinyal sepanjang jalur, setelah di track maka didapatkan hasil berupa file yang memiliki enkstensi berupa kml, file inilah data dari SSID yang telah berhasil di track yang kemudian dapat di buka melalui Google Earth. Pada percobaan kali ini , saya akann mentracking ke kawasan Puncak sekuning sampai Universitas Sriwijaya, Palembang.

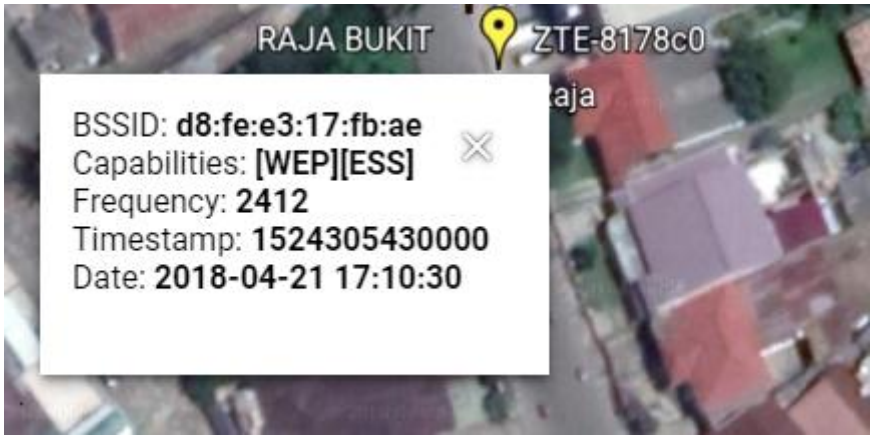
BAB IV
HASIL DAN ANALISIS PENGAMATAN

A. HASIL

Berikut adalah hasil dari tracking SSID yang sudah saya lakukan di sekitar kawasan Puncak Sekuning sampai Universitas Sriwijaya, Palembang

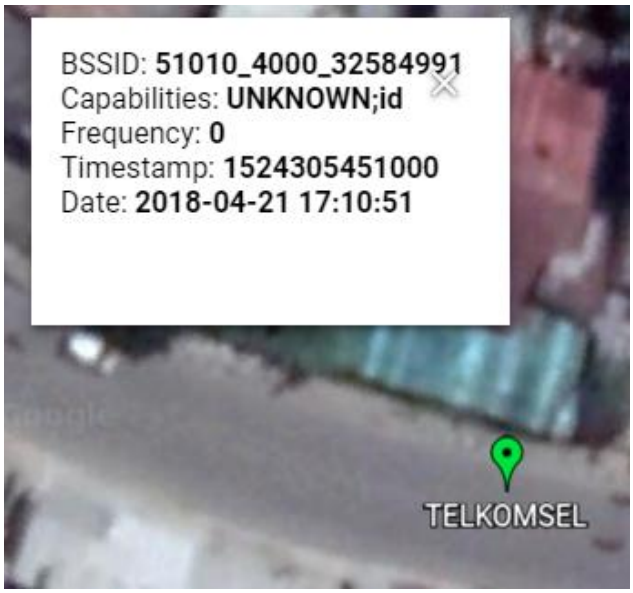


Gambar 1.



Gambar 2.

Gambar 3.



Gambar 4.

B. ANALISA

Setelah melakukan scanning di kawasan Puncak Sekuning – Universitas Sriwijaya didapatlah file format .kml yang kami export dari Wigle,dan saya langsung membuka file tersebut dengan menggunakan GoogleEarth, hasil yang didapat dari GoogleEarth adalah mapping yang bisa dilihat pada gambar diatas. Pada gambar diatas kita mendapatkan beberapa informasi seperti nama Wi-Fi apa saja yang ada di daerah yang kita lewati , SSID yang digunakan, Capabilities dan Frequency jaringan keamanan yang dipasang pada Wi-Fi tersebut.

Pada gambar diatas terlihat ada ikon berwarna merah, kuning dan hijau. Ikon berwarna merah menyatakan bahwa Access Point (AP) tersebut dilindungi oleh password dengan metode autentikasi WPA-PSK-CCMP dan menggunakan topologi berbasis ESS. Ini berarti jaringan SSID yang berwarna merah memiliki tingkat kerentanan akan peretasan jaringan sangatlah kecil atau bisa dibilang cukup aman karena memiliki keamanan jaringan dengan metode yang sangat aman seperti penggunaan konfigurasi PSK, hingga konfigurasi keamanan CCMP yang mampu merubah key secara dinamis pada masing masing WPA dan WPA2.

Ikon yang berwarna hijau menyatakan bahwa Access Point (AP) tersebut menggunakan metode autentikasi dengan servis RADIUS, SSID warna hijau tidak memiliki pengaturan keamanan jaringan wireless layaknya SSID pada warna merah, pada hal ini SSID berarti memiliki sifat terbuka pada seluruh device yang memperbolehkan mengakses jaringan tersebut sehingga SSID warna hijau memiliki kerentanan yang sangat besar akan aktifitas peretasan yang dilakukan oleh pihak pihak yang tidak bertanggung jawab.

Ikon kuning memiliki capabilities berupa informasi keamanan jaringan yang digunakan yaitu menggunakan keamanan jaringan dengan metode WEP dan informasi topologi jaringan yang digunakan yaitu ESS. Seperti yang dijelaskan pada dasar teori metode keamanan jaringan WEP ini kurang handal dibandingkan dengan WPA yang menggunakan PSK, CCMP dan TKIP. Keamanan WEP mudah untuk diretas karena menggunakan konfigurasi keamanan Shared key authentication yang bersifat statis, sehingga memudahkan pihak lain untuk membobol keamanan jaringan ini.

BAB V
KESIMPULAN

Dalam perkembangannya , keamanan jaringan wireless haruslah menjadi sesuatu yang diperhatikan, sebab , bahkan dengan menggunakan tools sederhana seperti wigle kemanan yang ada pada sebuah jaringan wireless akan sangat riskan. Semakin banyak upaya dari seorang hacker untuk membobol ataupun meretas sebuah jaringan wireless. Dalam pengamatan kali ini didapatlah kesimpulan yang tentunya berdasarkan apa yang terjadi dilapangan.

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. Pada pengamatan 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.