KEAMANAN JARINGAN KOMPUTER

War Driving Unsri Bukit Besar Sampai Jalan Masjid Al-Ghazali Palembang

Disusun oleh:

Nama : Rafli Eggy Ilham

NIM : 09011281520088

Dosen pengampuh : Deris Setiawan .M.T,Phd

Jurusan Sitem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2019

1. Pendahuluan

a. Wardriving

Wardriving adalah kegiatan di area tertentu melakukan pemetaan access point untuk tujuan statistik. Kemudian statistik ini digunakan untuk meningkatkan kesadaran akan masalah keamanan jaringan nirkabel (Joshua, 2007). Wardriving merupakan kegiatan explorasi tempat atau wilayah untuk exploitasi arau mendapatkan informasi mengenai jaringan wireless.

b. Wiggle

Wigle Wi-Fi adalah salah satu dari sekian banyak aplikasi yang digunakan untuk menjalankan kegiatan Wardriving. Aplikasi ini juga mudah untuk digunakan karena berbasis android dan free dan dapat di install melalui Google Play.

c. Google earth

Google Earth merupakan sebuah program globe virtual. Program ini memetakan bumi dari superimposisi gambar yang dikumpulkan dari pemetaan satelit, fotografi udara dan globe GIS 3D. Dengan program ini kita dapat mengaplikasikan file dari wigle berbentuk .kml kedalam peta di Google Earth.

d. Wap

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).

e. WPA PSK

WPA-PSK (Wi-Fi Protected Access – Pre Shared Key) adalah pengamanan jaringan nirkabel dengan menggunakan metoda WPA-PSK jika tidak ada authentikasi server yang digunakan. Dengan demikian access point dapat dijalankan dengan mode WPA tanpa menggunakan bantuan komputer lain sebagai server. Cara mengkonfigurasikannya juga cukup sederhana. Perlu diketahui bahwa tidak semua access point akan mempunyai fasilitas yang sama dan tidak semua access point menggunakan cara yang sama dalam mendapatkan Shared-Key yang akan dibagikan ke client. Pada access point Dlink DWL-2000AP, pemberian Shared-Key dilakukan secara manual tanpa mengetahui algoritma apa yang digunakan. Keadaan ini berbanding terbalik dengan akses point Linksys WRT54G, dimana administrator dapat memilih dari dua algoritma WPA yang disediakan, yang terdiri dari algoritma TKIP atau algoritma AES. Setelah Shared-Key didapat, maka client yang akan bergabung dengan access point cukup memasukkan angka/kode yang diijinkan dan dikenal oleh access point. Prinsip kerja yang digunakan WPA-PSK sangat mirip dengan pengamanan jaringan nirkabel dengan menggunakan metoda Shared-Key.

2. Pembahasan

2.1 alat dan bahan

-android smarphone

-software wiggle.net

-sofware google earth

2.2 wilayah

Kawasan depan unsri bukit besar sampai ujung jalan masjid Al-Ghazali

2.3 Langkah-Langkah Melakukan wardriving

1. Aktifkan jaringan Wi-fi dan paket data

2. Kemudian aktifkan GPS

3. Buka dan Aktifkan aplikasi wigle wifi

4. Pindai wilayah yang ingin di ambil informasinya dengan menelusi wilayah mana saja yang akan di wardring.

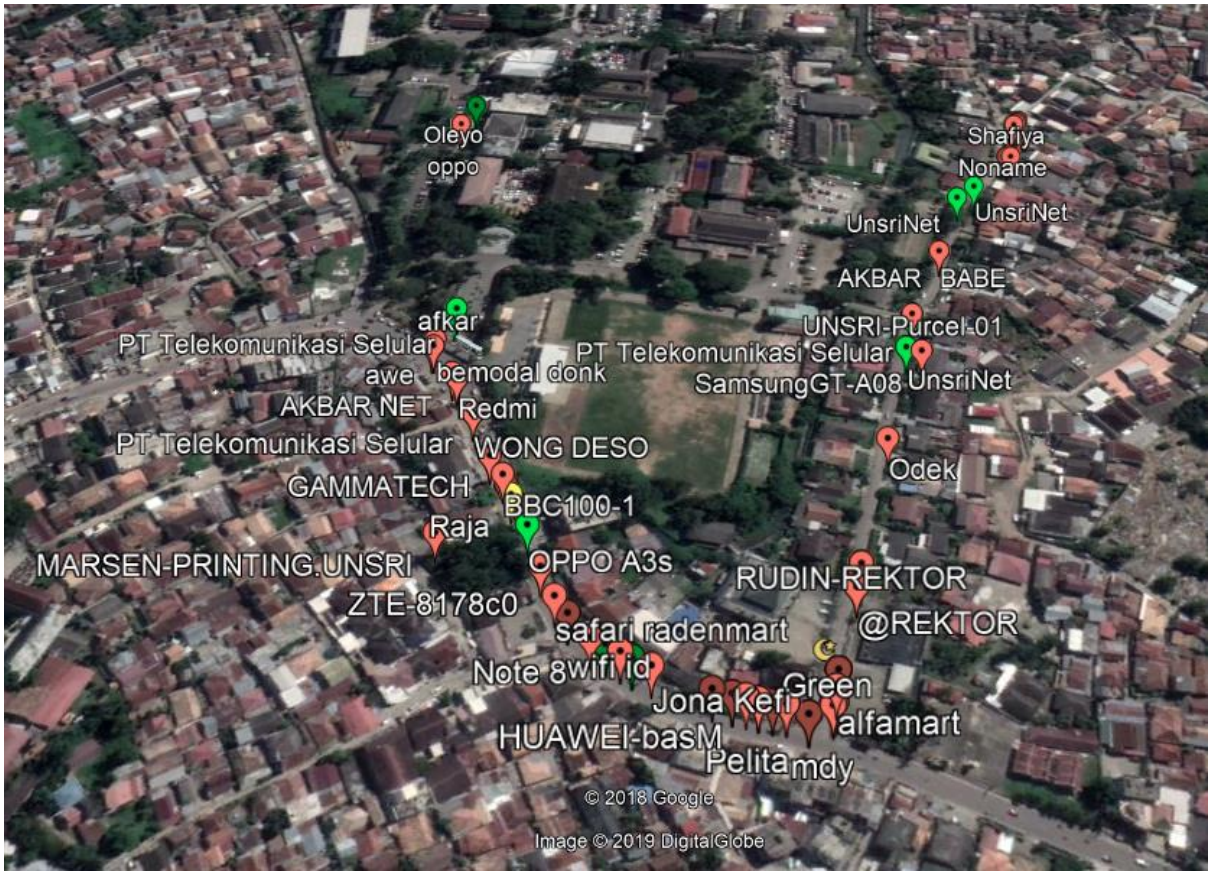
5. Setelah selesai, simpan data-data hasil pemindai dengan format kml

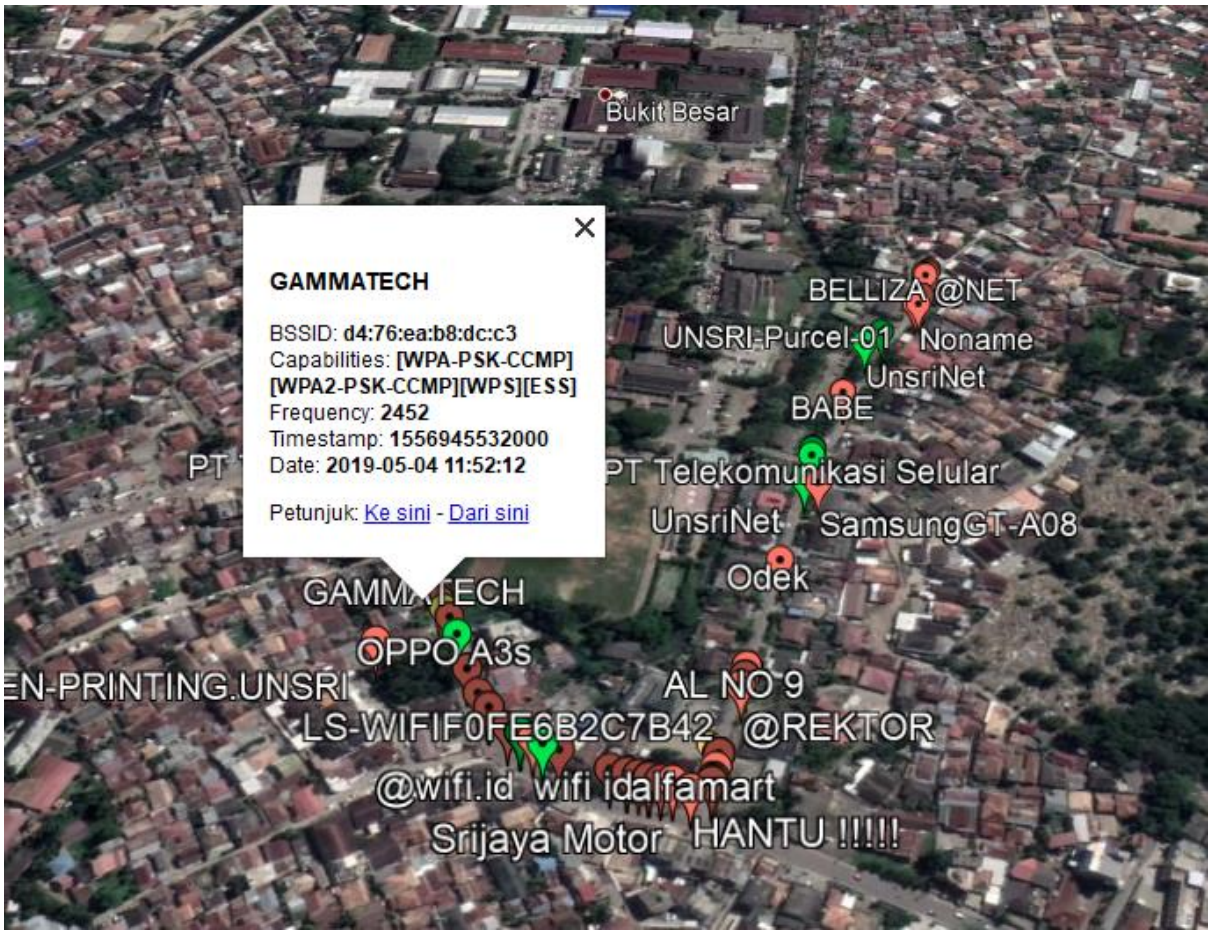
6. Buka aplikasi google eart kemudian impor data hasil pemindaian kml tadi, kemudian lakukan analilis.

2.4 hasil dan pembahasan

Dari gambar di bawah kita dapat mendapatkan informasi berupa network id, type encryption, time serta kekuatan sinyal dan accuracy. Network Id merupakan alamat dari router dan jaringan wireless tersebut sehingga jika ada orang jahat maka kode tersebut akan di masukan ke linux dengan bantuan aplikasi aircrack dan hasilnya akan mendapatkan akses berupa password untuk masuk kejaringan tersebut. Sedangkan type encryption adalah standar keamanan enkripsi yang dibuat untuk melindungi jaringan wireless dari serangan attacking. Pada Gambar terlihat access point tersebut menggunakan jenis enkripsi WPA2 yang merupakan perkembangan lebih lanjut dari WPA (Wireless Protected Acces). Selain mendapatkan informasi-informasi diatas, kita juga mendapatkan informasi berupa di daerah mana saja yang terdapat banyak jaringan wireless, bagaimana menghubungkan 1 cloud dengan cloud yang lainnya, bagaimana agar jaringan yang satu tidak saling tabrakan dengan informasi dari jaringan yang lainnya.

Pada gambar terdapat 3 warna pin yaitu warna hijau,kuning, dan merah. Yang berwarna hijau menandakan bahwa jaringan sinyal dari acces point itu kuat, yang berwarna kuning menandakan bahwa jaringan sinyal dari acces point itu sedang, dan Yang berwarna merah menandakan bahwa jaringan sinyal dari acces point itu lemah.


Oleyo
oppo
Shafiya
Noname
UnsriNet
UnsriNet
AKBAR
BABE
afkar
PT Telekomunikasi Selular
UNSRI-Purcel-01
PT Telekomunikasi Selular
awe
bemodal donk
SamsungGT-A08
UnsriNet
AKBAR NET
Redmi
PT Telekomunikasi Selular
WONG DESO
Odek
GAMMATECH
BBC100-1
Raja
MARSEN-PRINTING.UNSRI
OPPO A3s
RUDIN-REKTOR
ZTE-8178c0
@REKTOR
safari
radenmart
Note 8
wifi id
Green
Jona
Kefi
alfamart
HUAWEI-basM
Pelita
mdy
© 2018 Google
Image © 2019 DigitalGlobe


Bukit Besar
GAMMATECH
BSSID: d4:76:ea:b8:dc:c3
Capabilities: [WPA-PSK-CCMP] [WPA2-PSK-CCMP][WPS][ESS]
Frequency: 2452
Timestamp: 1556945532000
Date: 2019-05-04 11:52:12
Petunjuk: Ke sini - Dari sini
BELLIZA @NET
UNSRI-Purcel-01
Noname
UnsriNet
BABE
PT Telekomunikasi Selular
UnsriNet
SamsungGT-A08
Odek
OPPO A3s
AL NO 9
@REKTOR
@wifi.id
wifi id
alfamart
Srijaya Motor
HANTU !!!!!

3. Kesimpulan

Wardriving digunakan untuk memindai suatu wilayah yang memiliki jarigan wireless dan menganalisa keamanan dari sistem wireleess itu sendiri. Dengan dilakukannya wardring dapat di ketahui daerah atau titik mana saja yang ada jaringan wireless serta detail informasi jaringan wireless itu sendiri. Kegiatan wardriving dapat menggunakan berbagai aplikasi seperti wigle wifi,netstumble,istumbler,dan kismet.dan tak lupa juga untuk network mappingnya kita teteap menggunakan aplikasi tambahan seperti Google Earth. Dengan melakukan wardriving kita akan mendapatkan informasi seperti bagaimana kekuatan sinyal dari acces point tersebut,menggunakan tipe standar keamanan enkripsi jenis apa,waktu kita melakukan wardriving,mac addrees dari router jaring tersebut.Serta dapat mengetahui daerah mana yang sangat padat akan jaringan internet.