PEMETAAN WIRELESS ACCESS POINT USING GPS SMARTPHONE ANDROID MENGGUNAKAN METODE WARDRIVING

Dikka Pratama[1], Merry Agustina, MM, M.Kom[2], Hadi Syaputra, S.Kom[3]

Mahasiswa Informatika[1], Dosen Fakultas Ilmu Komputer Universitas Bina Darma[2,3]
Jalan Jenderal Ahmad Yani No.12 Palembang
Pos-el : Pratama_dikka@yahoo.co.id[1],merry_agustin@mail.binadarma.ac.id[2], Hady_syaputra@mail.binadarma.ac.id[3]

Abstrak. Perkembangan jaringan *teknologi nirkabel* saat ini berkembang dengan pesat dan hampir dapat ditemui disetiap tempat sepeti kafe, perguruan tinggi, perkantoran, supermarket, ataupun perumhan daerah. Pengguna dengan mudah membuat koneksi ke *jaringan internet* dengan *jaringan nirkabel* tanpa bantuan kabel karena data akan disiarkan melalui *frekuensi* radio. Perkembangan jaringan computer ditempat umu terkadang memberikan laynan khusus, terutama *jaringan nirkabel gratis (free hotspot). Jaringan nirkabel (wireless)* yang bersifat broadcast membuat komunikasi data yang terjadi cendrung tidak aman dan memang pengguna menyampingkan *issue security* pada *IEEE 802.11* sehingga banyak *intruders* yang memfokuskan serangannya pada *protocol* satu ini. Sebut saja *wardriving atau craking WPA/WEP/WPA2, MitM (Man in the Middle Attack)* bahkan membuat *dumpy access point* yang digabung dengan *client-side exploit dan MiTM pada protocol https*.

Kata kunci : *wireless, wardriving security, hacking,* Palembang

Abstract. The development of wireless network technology is currently growing rapidly and can be found almost every place such as cafes, colleges, offices, supermarkets, or even residential areas. Users can easily create a connection to the internet network with a wireless network without wires because the data will be broadcast via radio frequency. The development of computer network in public places sometimes provide special services, especially the free wireless network (free hotspot). Wireless network (LAN) that is broadcast makes data communications than occur tend to be insecure and indeed users generally exclude the issue of security on the IEEE 802.11 so many intrudes are focusing their attacks on one's protocol. Call in wardriving or craking WPA/WEP/WPA2 MitM (Man in the Middle Attack) even made a dummpy access point combined with client-side exploits and MitM the https protocol.

Password: wireless, wardriving security, security, hacking, Palembang.

1. PENDAHULUAN

Seiring dengan perkembangan *IPTEK* pada saat ini juga berpengaruh pada perkembangan teknologi jaringan komputer, dimana teknologi jaringan komputer yang menggunakan media *signal* yang memanfaatkan gelombang radio sebagai media komunikasinya.

Teknologi jaringan nirkabel atau *wireless* yang banyak digunakan diberbagai tempat adalah *wi-fi*. Istilah *wi-fi* diciptakan oleh sebuah organisasi yang bernama *wi-fi alliance* yang menguji sertifikasi perangkat-

perangkat *wireless LAN* sedangkan kode *802.11* adalah nomor *standarisasi* dari sistem *wireless LAN.*

Pemanfaatan jaringan *nirkabel wireless* yang bersifat *broadcast* membuat komunikasi data cendrung tidak aman, dan memang pengguna umumnya menyampingkan *issue security IEE 802.11.* sehingga banyak *intruders* yang memfokuskan serangan *protokol* satu ini. Sebut saja *wardriving* atau *craking WPA/WEP/WPA2.*

Mengetahui permasalahan pada jaringan *wireless* dan padatnya *channel wireless* di kota besar, sehingga mendorong penulis untuk berupaya memetakan lokasi *access point* di wilayah kota Palembang dan menjelaskan metode ataupun cara yang digunakan oleh *intruders* baik itu cari yang bersifat terbuka ke *public* ataupun yang masih bersifat *pribadi* dan Juga cara untuk meminimalisir serangan dari *intruders* tersebut.

Dari Permasalahan yang ada pada latar belakang diatas, maka penulis akan merumuskan penelitian dengan judul ***"Pemetaan Wireless Access Point Using Gps SmartPhone Android Dengan Metode Wardriving Di Kota Palembang".***

Metode Penelitian

Metode Penelitian Tindakan *(Action Research)*

Dalam rangka penyelesaian penelitian ini maka digunakan metode penelitian tindakan (*Action Research*).

Berikut tahapan penelitian tindakan (*Action Research)* yang dapat ditempuh :

1.Melakukan diagnosa *(diagnosing*)

Melakukan identifikasi masalah-masalah pokok yang ada guna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan.

2.Membuat Rencana Tindakan (*action planning*)

Penulis memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada.

3.Melakukan tindakan (*Action Taking*)

Penulis mengimplementasikan rencana tindakan dengan harapan dapat menyelesaikan masalah.

4.Melakukan Evaluasi (*evaluating*)

Setelah masa implementasi *(Action Taking)* dianggap cukup kemudian penulis melaksanakan evaluasi hasil dari *implementasi* dalam tahap ini dilihat bagaimana pengguna yang ditandai dengan berbagai aktifitas.

5.Pembelajaran *(Learning*)

Tahap ini Merupakan bagian akhir siklus yang telah dilalui dengan melaksanakan *review* tahap-pertahap yang telah berakhir kemudian penelitian in berakhir.

Metode Pengujian

Metode yang digunakan adalah Metode *Wardriving* dimana dalam melakukan *wardriving* membutuhkan aplikasi-aplikasi pendukung dilaptop seperti kismac, Giskismet, GPSD, untuk menjalankan nya menggunakan Linux atau backtrack, aplikasi-aplikasi pendukung di *Android* seperti *blueNMEA, Wifi Analyzer, Wigle Wifi*.

2.1 Landasan Teori

2.1.1 Wireless Dan Sejarahnya

Wireless adalah *transfer* informasi antara dua atau lebih titik yang tidak terhubung secara fisik. Jarak bisa pendek, seperti beberapa meter untuk *remote control* televisi, atau sejauh ribuan atau bahkan jutaan kilometer untuk ruang-dalam *komunikasi radio.*

Wireless pertama pada tahun 1970-an. didahului oleh IBM dengan rancangan teknologi RI, dan perusahaan HP, dengan ISM band yaitu 902-908 Mhz, 2400+2483 dan 5725-5850 Mhz, pada tahun 1990 dipasarkan dengan teknik *spektrum* tersebar (SS) pada pita ISM, terlisensi *frekuensi* 18-19 Ghz, pada tahun 1997 *IEEE* membuat *standar WLAN* dengan kode 802.11 dapat bekerja pada *frekuensi* 2.4 Ghz kecepatan 2 Mbps ,pada juli 1999 *IEEE* kembali mengeluarkan kode 802.11b dengan kecepatan 11 Mbps dan pada waktu hampir bersamaan *IEEE* juga mengeluarkan 802.11a menggunakan *frekuensi 5 Ghz*, dan kecepatan data hingga 54Mbps. Tahun 2002 *IEEE* menggabungkan kelebihan 802.11b dan 802.11a yakni 802.11g bekerja pada f*rekuensi 2.4 Ghz* hingga 54Mbps. Yang terkhir tahun 2006 *IEEE* mengeluarkan teknologi 802.11n dikembangkan dengan menggabungkan 802.11b dan 802.11g sehingga menghasilakan peningkatan *throughput* dengan kecepatan 108Mbps (James, 2009).

2.1.2 Keamanan Jaringan

Network Security pada awalnya konsep ini menjelaskan lebih banyak mengenai keterjaminan (*security*) dari sebuah sistem jaringan komputer yang terhubung ke internet terhadap ancaman dan gangguan yang ditunjukan kepada sistem tersebut. *Network Security* hanyalah menjelaskan kemungkinan-kemungkinan yang akan timbul dari *konektivitas* jaringan komputer lokal kita dengan *wide-area network.*

Secara Umum, terdapat 3 (tiga) kata kuncin dalam konsep *network security* ini,yaitu:

- resiko/tingkat bahaya
- ancaman,dan
- kerapuhan sistem (*vulnerability*)

2.1.2.1 Resiko atau tingkat bahaya

Dalam hal ini,resiko berarti berap besar kemungkinan keberhasilan para penyusup dalam rangka memperoleh akses ke dalam jaringan komputer lokal yang memiliki *konektivitas* jaringan *local* ke *wide-area network.*

Secara umum akses-akses yang diinginkan adalah:

- *Read Acces* : mampu mengetahui keseluruhan sistem jaringan informasi.
- *Write Acces* : Mampu melakukan proses menulis ataupun menghancurkan data yang terdapat pada sistem tersebut.
- *Denial Of Service* : Menutup penggunaan utilitas-utilitas jaringan normal dengan cara menghabiskan jatah *CPU, bandwidth* maupun *memory.*

2.1.2.2 Acaman

Dalam hal ini ,ancaman berarti orang yang berusaha memperoleh akses-akses *ilegal*

terhadap jaringan komputer yang dimiliki seolah-olah ia memiliki *otoritas* terhadap akses ke jaringan komputer.

2.1.2.3 Kerapuan System (*Vulnerabity*)

Kerapuhan sistem lebih memiliki arti seberapa jauh proteksi yang bisa diterapkan kepada *network* yang dimiliki dari seseorang dari luar sistem yang berusaha memperoleh akses ilegal terhadap jaringan komputer tersebut dan kemungkinan orang-orang dari dalam sistem memberikan akses kepada dunia luar yang bersifat merusak sistem jaringan.

Untuk menganalisa sebuah sistem jaringan informasi *global* secara keseluruhan tentang tingkat keandalan dan keamanannya bukanlah suatu hal yang mudah dilaksanankan. Analisa terhadap sebuah sistem jaringan informasi tersebut haruslah mendetail mulai dari tingkat kebijaksanaan hinga tingkat aplikasi praktisnya

2.1.3 Mekanisme Keamanan Wireles

2.1.3.1 WEP

WEP merupakan *standart* keamanan & *enkripsi* pertama yang digunakan pada *wireless*, *WEP* (*Wired Equivalent Privacy*) adalah suatu metode pengamanan jaringan *nirkabel*, disebut juga dengan *Shared Key Authentication. Shared Key Authentication* adalah *metode 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 *access point* ke *client*, dengan yang dimasukkan *client* untuk authentikasi menuju *access point*, dan *WEP* mempunyai standar 802.11b.

2.1.3.2 WPA

Menyikapi kelemahan yang dimiliki oleh *WEP*, telah dikembangkan sebuah teknik pengamanan baru yang disebut sebagai *WPA (WiFI Protected Access*). Teknik *WPA* adalah model *kompatibel* dengan *spesifikasi standar draf IEEE 802.11i.* Teknik ini mempunyai beberapa tujuan dalam desainnya, yaitu kokoh, *interoperasi,* mampu digunakan untuk menggantikan *WEP,* dapat diimplementasikan pada pengguna rumahan atau *corporate*, dan tersedia untuk *publik* secepat mungkin. Adanya *WPA* yang "menggantikan" *WPE*, apakah benar perasaan "tenang" tersebut didapatkan? Ada banyak tanggapan pro dan kontra mengenai hal tersebut. Ada yang mengatakan, *WPA* mempunyai *mekanisme enkripsi* yang lebih kuat. Namun, ada yang *pesimistis* karena alur komunikasi yang digunakan tidak aman, di mana teknik *man-in-the-middle* bisa digunakan untuk mengakali proses pengiriman data. Agar tujuan *WPA* tercapai,setidaknya dua pengembangan sekuriti utama dilakukan. Teknik *WPA* dibentuk untuk

menyediakan pengembangan *enkripsi* data yang menjadi titik lemah *WEP,* serta menyediakan *user authentication* yang tampaknya hilang pada pengembangan konsep *WEP*

2.1.3.3 WPA2

WPA2 adalah *sertifikasi produk* yang tersedia melalui *Wi-Fi Alliance*. *WPA2 Sertifikasi* hanya menyatakan bahwa peralatan *nirkabel* yang *kompatibel* dengan *standar*

IEEE 802.11i. WPA2 sertifikasi produk yang secara resmi menggantikan *wired equivalent privacy (WEP)* dan fitur keamanan lain yang asli *standar IEEE 802.11*. *WPA2* tujuan dari *sertifikasi* adalah untuk mendukung wajib tambahan fitur keamanan *standar IEEE 802.11i* yang tidak sudah termasuk untuk produk-produk yang mendukung *WPA*.

2.1.4 Definisi Wardriving

Wardriving merupakan aktifitas bergerak di sekitar area tertentu, melakukan pemetaan *access point* untuk tujuan *statistik*. Kemudian *statistik* ini digunakan untuk meningkatkan kesadaran akan masalah keamanan yang terkait dengan *wireless* (Joshua, 2007).

2.1.5 Sejarah Wardriving

Istilah *wardriving* berasal dari *Wardialing*, sebuah istilah yang pertama kali diperkenalkan ke *public* oleh *Matthew Broderick, David Lightman* di *film wargames(1983)*. *wardialing* merupakan praktek menggunakan modem *telephone* yang terpasang ke *computer* untuk melakukan dial ke seluruh nomor secara berurutan (misal 555-111, 555-112 dan seterusnya) untuk mencari komputer yang terhubung dengan modem yang menyertainya. Pada dasarnya *wardriving* menggunakan konsep yang sama, meskipun teknologi terus berkembang seperti saat ini. Seorang *wardiving* sering melakukan pemetaan route yang akan di lewati terlebih dahulu, untuk menemukan *access point wireless* di daerah tersebut. Setelah *access points wireless* ditemukan seorang *wardriver* menggunakan *software dan website* untuk memetakan hasilnya. Berdasarkan hasil tersebut, dilakukan analisis *statistik*. *Statistik* analis dapat dilakukan seper-area, seperdaerah ataupun keseluruhan dari *wireless* tersebut (Joshua, 2007).

2.1.6 Pemetaan

Pemetaan adalah pengelompokkan suatu kumpulan wilayah yang berkaitan dengan beberapa letak *geografis* wilayah yang meliputi dataran tinggi, pegunungan, sumber daya dan potensi penduduk yang berpengaruh terhadap sosial kultural yang memilki ciri khas khusus dalam penggunaan skala yang tepat. *(Soekidjo,1994)*.

Pengertian lain tentang pemetaan yaitu sebuah tahapan yang harus dilakukan dalam pembuatan peta. Langkah awal yang dilakukan dalam pembuatan data, dilanjutkan dengan pengolahan data, dan penyajian dalam bentuk peta *(Juhadi dan Liesnoor, 2001)*.

Jadi, dari dua *definisi* diatas dan disesuaikan dengan penelitian ini maka pemetaan merupakan proses pengumpulan data untuk dijadikan sebagai langkah awal dalam pembuatan peta, dengan menggambarkan penyebaran kondisi alamiah tertentu secara meruang, memindahkan keadaan sesungguhnya kedalam peta dasar, yang dinyatakan dengan penggunaan skala peta.

2.1.7 Android

Android Merupakan sebuah sistem operasi yang berbasis Linux untuk telepon seluler seperti telepon pintar dan komputer tablet. *Android* menyediakan platform terbuka bagi para pengembang untuk menciptakan

aplikasi mereka sendiri untuk digunakan oleh bermacam peranti bergerak.

Awalnya, *Google Inc.* membeli *Android Inc.*, pendatang baru yang membuat peranti lunak untuk ponsel. Kemudian untuk mengembangkan *Android*, dibentuklah *Open Handset Alliance*, *konsorsium* dari 34 perusahaan peranti keras, peranti lunak, dan *telekomunikasi*, termasuk *Google, HTC, Intel, Motorola, Qualcomm, T-Mobile,* dan *Nvidia*. Pada saat perilisan perdana *Android*, 5 November 2007, *Android* bersama *Open Handset Alliance* menyatakan mendukung pengembangan standar terbuka pada perangkat seluler. Di lain pihak, *Google* merilis kode–kode *Android* di bawah *lisensi Apache*, sebuah *lisensi* perangkat lunak dan *standar* terbuka perangkat *seluler*.

Di dunia ini terdapat dua jenis distributor sistem operasi *Android*. Pertama yang mendapat dukungan penuh dari *Google atau Google Mail Services (GMS)* dan kedua adalah yang benar–benar bebas distribusinya tanpa dukungan langsung Google atau dikenal sebagai *Open Handset Distribution (OHD)*

2.1.8 Sejarah android

Sejarah *android* pada mulanya berasal dari perusahaan bernama *Android, Inc.* didirikan tempatnya di *Palo Alto, California*, pada Oktober tahun 2003 oleh Andy Rubin (pendiri Danger), *Rich Miner* seorang pendiri *Wildfire Communications, Inc., Nick Sears* seorang mantan *VP T-Mobile*, dan *Chris White* seorang kepala desain dan pengembangan antarmuka *WebTV* untuk mengembangkan sebuah "perangkat seluler pintar yang lebih sadar tentang lokasi dan *preferensi* penggunanya". Tujuan awal dari perkembangan tersebut pada mulanya diperuntukkan bagi *kamera digital*, namun disadari bahwa pasar dari *kamera digital* tidak besar potensinya, dan pengembangan *Android* lalu dialihkan pada pasar telepon pintar atau *smartphone* untuk menyaingi *Symbian* serta *Windows Mobile (iPhone Apple* pada saat itu belum dirilis).

Meskipun para pengembang *Android* tersebut merupakan pakar-pakar teknologi yang berpengalaman, *Android Inc*. dijalankan secara diam-diam dan hanya diungkapkan bahwa para pengembang tersebut sedang berusaha menciptakan sebuah perangkat lunak yang dapat diperuntukkan untuk telepon seluler. Masih pada tahun yang sama, *Andy Rubin* kehabisan uang. *Steve Perlman* adalah seorang teman dekat *Andy Rubin* dan meminjaminya $10.000 tunai serta menolak tawaran saham di perusahaan.

Google mengakuisisi perusahaan *Android Inc*. pada tanggal 17 Agustus 2005 dan menjadikannya sebagai anak perusahaan yang dimiliki oleh Google. Pendiri *Android Inc.* yaitu *Rubin, Miner, serta White* tetap bekerja pada perusahaan tersebut setelah diakuisisi oleh *Google*. *Di Google*, tim yang dipimpin oleh *Andy Rubin* mulai untuk mengembangkan sebuah *platform* perangkat seluler dengan menggunakan *kernel Linux*.

Sejak tahun 2008, *Android* mulai secara bertahap melakukan sejumlah pembaruan atau *update* untuk meningkatkan

kinerja dari sistem operasi tersebut dengan menambahkan fitur baru, memperbaiki *bug* pada *versi android* yang sebelumnya. Setiap versi yang dirilis dinamakan secara *alfabetis* dengan berdasarkan nama sebuah makanan pencuci mulut, seperti cupcake, donut, dan sebagainya.

3. METODOLOGI

Dalam penelitian ini terdapat beberapa variabel yaitu:

- Variabel bebas *(independen)*

Variable ini sering disebut sebagai *variabel predictor*, variabel pengaruh, kausa, variabel perlakuan, *treatment*, variabel risiko, *stimulus*, dan juga dikenal sebagai variabel bebas.

Variabel ini merupakan variabel yang menjadi sebab terjadinya perubahan atau mempengaruhi timbulnya variabel terikat *(dependen)*. Oleh karena itu, variabel ini disebut variabel bebas *(independent)*. Variabel bebas juga sering tuliskan dalam *Structural Equation Modelling* sebagai *variabel eksogen.*

Dalam variable ini dibutuhkan software dan hardware yang akan digunakan untuk *wardriving*

- Variable terikat *(dependen)*

sering disebut sebagai *variabel konsekuen*, variabel kriteria, variabel pengaruh,
terikat, tergantung, dan *variabel output.*

Berbeda dengan *variabel independet*, *variabel dependen* dalam SEM atau

permodelan persamaan *struktural*, *variabel independen* juga dikenal sebagai *variabel indogen.*

Alasan *variabel dependen* disebut variabel terikat adalah karena setiap variabel *independen* akan mempengaruhi variabel terikat / *independen.*

Dalam variable ini merupakan hasil dari penelitian yang telah dilakukan peneliti

- Variabel kontrol

Variable control merupakan variabel yang dikendalikan atau dibuat konstan sehingga hubungan variabel bebas terhadap variabel terikat tidak dipengaruhi oleh faktor dari luar yang tidak diteliti.

Variabel kontrol sering dipakai oleh peneliti dalam penelitian yang bersifat membandingkan, melalui penelitian *eksperimental.*

Dalam variable ini adalah tempat dimana peneliti melakukan penelitian yaitu di wilayah kota Palembang

3.2 Peralatan Yang Di Butuhkan

1. *Wardriving* menggunakan mobil

Hardware:

- *Laptop Asus*
- *Wireless USB*
- *GPS system* dengan *Bluetooth*.

Software :

- *Kismet, Kismac*

Kismet adalah 802,11 *layer2 detektor* jaringan *nirkabel,sniffer*, dan *system deteksi intrusi*. *Kismet* akan bekerja dengan kartu nirkabel yang mendukung *monitoring* mode(rfmon) baku, dan (dengan hardware yang sesuai) dapat mendukung plugin yang memungkinkan *sniffing* meda lain seperti DECT

Kismet mengidentifikasi jaringan bernama standar,mendeteksi (dan diberi waktu, *decloaking*) jaringan tersembunyi dan inferring kehadiran *nonbeaconing* jaringan melalui lalu lintas data

- *Gpsd (*menghubungkan *gps bluetooth* ke laptop)
- *BlueNMEA*(*software bluetooth gps* pada *android*)

BlueNMEA adalah sebuah aplikasi *Android* yang mengirimkan data lokasi melalui *Bluetooth (RFCOMM)* atau *TCP* dalam format *NMEA.*

2.*Wardriving* menggunakan *smartphone*

Hardware :

- *Samsung V / Tablet ASUS*

Software :

- *Wigle.wifi*
- *Wifi analyzer*

3.3 Pemilihan Antena

Secara umum antena dibagi menjadi 2 macam yaitu :

- *Omnidirecitonal*
- *Directional*

Omnidirecitonal : Antena ini akan memancarkan dan menangkap sinyal atau frekuensi radio dari dan ke segala arah. berbeda dengan *antena omni, directional* berbentuk seperti parabola dan sifatnya mengumpulkan dan mengirimakan signal dalam satu arah. Dikarenakan dalam kasus ini digunakan untuk proses *wardriving* maka yang dipilih adalah *antena omni,* sifatnya yang memancarkan dalam bentuk kesegala arah memberikan keuntungan dalam proses *scanning access point.*

3.4 Metode Pengumpulan Data

Adapun teknik yang digunakan untuk pengumpulan data adalah

1. Observasi

Dimana pada metode ini peneliti mengumpulkan data dengan cara terjun langsung ke area-area yang menggunkan *wireless* untuk mengetahui *wireless* apasaja yang digunakan dikota Palembang.

2. Metode studi keputusan

Yaitu dengan cara mengumpulkan data-data yang dilakukan dengan membaca,mempelajari buku-buku dan jurnal-jurnal yang berkaitan dengan permasalahan yang akan menunjang terhadap materi pembahasan masalah yang diteliti.

3.5 Jenis Dan Sumber Data

Data-data yang dibutuhkan dalam penelitian ini terdiri dari data *primer* dan data *skunder*.

1. Data *Primer*

Data yang diperoleh secara langsung dari objek penelitian yang dilakukan oleh peneliti diwilayah kota Palembang

2. Data *skunder*

Data yang diperoleh secara tidak langsung, yang didapatkan dari data atau arsip peneliti sebelumnya.

3.6 Prosedur Penelitian

Secara umum prosedur penelitian dibagi menjadi dua yaitu :

1. Tahap persiapan

   Pada tahap ini yang akan dilakukan adalah :

a. Menentukan jadwal penelitian
b. Mempelajari cara-cara untuk melakukan Pemetaan *wireless access point using gps smartphone android*
c. Mempersiapkan rancangan penelitian (RPP).

2. Tahap pelaksanaan

   Pada tahap ini yang dilakukan adalah :

a. Menjalankan semua aplikasi-aplikasi yang akan digunakan dalam pemetaan *wireless acces point using gps smartphone android* menggunakan metode *wardriving*
b. Setelah semua aplikasi dijalankan baru lah melakukan proses *wardriving* diberbagai tempat dikota Palembang yang mungkin mempunyai *wireless*
c. Uji coba *wardriving* menggunakan *Wigle.wifi* di *Android*

Dari percobaan menggunakan *wiggle.wifi* di *Android* terdapat *343 wireless* yang terdeteksi disebagian kecil wilayah kota Palembang, pada saat salah satu *wireless* yang terdeteksi di *wigle.map* diklik maka akan tampil seperti gambar Dibawah ini.

Gambar 3.1 wigle.map

3.7 Pemilihan Sistem Operasi

Pemilihan Sistem Operasi dalam melakukan proses wardriving sangat fatal,
dikarenakan mempengaruhi tools yang akan digunakan dan hasil yang akan di dapatkan. Sistem Operasi berbasis open source lebih fleksibel, lebih akurat dalam penyajian data.

3.8 Proses Wardriving

1. langkah-langkah wardriving menggunakan laptop
   a. wardriving menggunakan backbox
   b. install BlueNMEA
   c. jalankan GPSD terlebih dahulu untuk koneksi GPS Android Ke Laptop
   d. Aktifkan mode Mon0 dan Jalankan *kismet*

e. Masukan *interface* "Mon0"

f. Jalankan *kismet_client*, jika *GPS*nya telah terkoneksi

g. Melakukan *giskismet* dimana langkah ini untuk mengubah *file* log hasil *monitoring kismet* menjadi KML format diintegrasikan ke *google map*.

h. Mapping with google earth

1. Langka-langkah *Wardiving* menggunakan *smartphone android*

   a. Menggunakan aplikasi *wigle wifi wardriving dari wigle.net*
   b. *Aktivasi Gps dan wireless*
   c. Jalankan aplikasi dan lakukan proses *wardriving*

4. HASIL

Hasil dari Pemetaan wireless access point using gps smartphone android menggunkan metode Wardriving

Gambar 4.3 Pemetaan wireless access point

Gambar 1 diatas adalah hasil dari Pemetaan wireless access point using gps smartphone android menggunkan metode Wardriving di Kota Palembang, dapat dilihat bahwa terdapat banyak access point yang digunakan diberbagai daerah di kota Palembang

.

5. KESIMPULAN

5.1 Kesimpulan

Dari penjelesan dan pembahasan dari hasil penelitian yang dilaksanakan di kota Palembang dengan judul "Pemetaan *wireless access point using gps smartphone android* menggunakan *metode wardriving*" maka dapat diambil kesimpulan sebagai berikut :

1. Wilayah kota Palembang yang memiliki *jaringan wireless* yang paling padat yakni wilayah kampus, Perkantoran, Rumah Sakit, Supermarket, minimarket.

2. Untuk *Enkripsi Jaringan Wireless* di Kota Palembang cukup baik karena Masyarakat umum sudah menyadari tingkat *keamanan jaringan wireless* sangatlah penting.
3. *Interferensi Channel* pada wilayah Kota Palembang rendah karena 19% masih terjadi *interferensi* ini menunjukan bahwa *user* sudah mengetahui channel yang tepat agar terhindar dari interferensi sehingga *performance wireless* akan menjadi lebih baik.
4. Untuk mengurangi resiko keamanan *jaringan wireless user* bisa mensetting *access point*, mengganti *password default*, dan mengganti *enkripsi* yang lebih baik yakni *wpa/wpa2*

5.2 Saran

Berdasarkan analisa hasil *wardriving* dan keamanan dalam *jaringan wireless* makan saran pengembangan selanjutnya dalam bidang ini antara lain :

1. pada penelitian berikutnya pengambilan data *wardriving* dilengkapi karena peneliti yang sekarang hanya mengambil titik dibeberapa tempat atau jalan saja.
2. Melakukan *wardriving diarea* yang lebih luar agar didapatkan hasil yang semakin lengkap
3. Mengevaluasi keamanan jaringan wireless dengan *mensimulasikan* serangan dari *attacker*
4. Menggunakan *devices* yang lebih mendukung dalam *scanning frekuensi jaringan wireless*

DAFTAR RUJUKAN

1. Chandra. 2008 Penelitian tindakan (*action research*) *https://chandrax.wordpress.com/2008/07/05/action-research-penelitian tindakan/*
2. Ismayudi. 2014 " Analisis Keamanan jaringan WIFI SMPN 1 Sembawa'' *http://eprints.binadarma.ac.id/164/* diakses pada tanggal 20 january 2014
3. Juhadi dan Liesnoor, 2001 Pengertian Pemetaan PengetahuanPintar.blogspot.com.Sejarah Wireless *http://pengetahuanpintars.blogspot.com/2011/12/sejarah-wireless-dan pengertiannya.html*
4. Reza Jalaluddin Al-Haroh. 2012 "Wardriving dan Penetrasi wifi lanjut di wilayah kota Yogyakarta'' *http://repository.amikom.ac.id/files/publikasi_08.11.2153.pdf*
5. Tedi Wahyono. 2012 "Analisis Pemetaan Jaringan *HotsPot* Di Perpustakaan Daerah (PUSDA) Provinsi Sumatera Selatan" *http://eprints.binadarma.ac.id/424/*
6. Soekidjo,1994 Pengertian Pemetaan
7. Wright Joshua 2007. Wardriving dan Penetration Testing.