ANALISIS KEAMANAN JARINGAN *WIRELESS* MENGGUNAKAN METODE *WARDRIVING* PADA KANTOR PEMERINTAH KOTA PRABUMULIH

Hidayat Eral Putra[1], Alex Wijaya[2], RM Nasrul Halim[3]

Mahasiswa Teknik Informatika[1], Dosen Fakultas Ilmu Komputer Universitas Bina Darma[2,3]
Jalan Jenderal Ahmad Yani No.12 Palembang
Email : saka_distraction@yahoo.com

Abstract : Wireless network has been used as an excellent internet provider. By utilizing a wireless network, users can enjoy the internet without having to connect a cable. Prabumulih Government already using Wireless as an internet provider that can be used by employees who already have a login. Wireless networks are good must have good security in order to avoid the threat of crime. Wardriving, is an activity in which a person or group of people equipped with the tools and expertise to access a wireless network for free or without login. Wardriving is a threat to the government Prabumulih for important data that is processed using a wireless network is not secured. To find out how strong the security of wireless networks at government offices Prabumulih, the necessary analysis. From the analysis that has been done, the result are wireless network at the municipal office prrabumulih not safe because there is still a hotspot point can do crack.

Keywords: *Wireless, Wardriving, Prabumulih*

Abstrak *:* Jaringan *Wireless* selama ini digunakan sebagai penyedia internet yang sangat baik. Dengan memanfaatkan jaringan *Wireless*, pengguna dapat menikmati internet tanpa harus tersambung pada sebuah kabel. Pemerintah kota prabumulih sudah menggunakan *Wireless* sebagai penyedia internet yang dapat digunakan oleh pegawai yang sudah memiliki *login*. Jaringan *Wireless* yang baik haruslah memiliki keamanan yang baik agar terhindar dari ancaman kejahatan. *Wardriving*,adalah suatu kegiatan diamana seseoran maupun sekelompok orang yang dibekali alat dan keahlian untuk mengakses sebuah jaringan *Wireless* secara gratis atau tanpa melakukan *login*. *Wardriving* merupakan ancaman bagi pemerintah kota prabumulih karena data penting yang diolah menggunakan jaringan *Wireless* tidak terjamin keamanannya. Untuk mengetahui seberapa kuat keamanan jaringan *Wireless* pada kantor pemerintah kota prabumulih, maka diperlukan analisis. Dari hasil analisis yang telah dilakukan, didapatlah kesimpulan bahwa jaringan wireless pada kantor pemerintah kota prrabumulih tidak aman karena masih ada titik *hotspot* yang dapat dilakukan *crack*.

Kata kunci*: Wireless, Wardriving,* Prabumulih

---

1. PENDAHULUAN

Jaringan *wireless* pada era digital saat ini sudah menjadi kebutuhan penting bagi suatu lembaga, jaringan *wireless* memudahkan para penggunanya untuk memperoleh internet yang dapat digunakan dalam memperoleh informasi. Pada suatu perusahaan atau perkantoran tentu mempunyai jaringan *wireless* yang diproteksi oleh keamanan, seperti menggunakan *user name* dan *password* untuk *login* agar dapat menggunakan jaringan *wireless* tersebut. Keberadaan jaringan *wireless* yang luas menimbulkan niat bagi orang atau sekelompok orang untuk mendapatkan jaringan *wireless* tersebut secara gratis ataupun dimanfaatkan untuk memperoleh data dari suatu lembaga maupun merusaknya.

Pada kantor pemerintahan kota prabumulih memiliki jaringan *wireless* yang berfungsi sebagai penyedia internet bagi pegawai yang akan digunakan untuk memperoleh informasi dan pengolahan data. Dinas Perhubungan Komunikasi dan Informatika (KOMINFO) merancang dan mengelolah *website* resmi Pemkot Prabumulih menggunakan jaringan *wireless*, tentunya penting menjaga suatu *web*site agar tidak dirusak oleh orang yang tidak bertanggung jawab. Jaringan *wireless* pada kantor pemerintahan kota prabumulih cukup besar sehingga memungkinkan untuk melakukan *wardriving*.

Wardriving adalah kegiatan atau aktivitas untuk mendapatkan informasi tentang suatu jaringan *wireless* dan mendapatkan akses terhadap jaringan *wireless* tersebut. Umumnya bertujuan untuk mendapatkan koneksi internet, tetapi banyak juga yang melakukan *wardriving* untuk maksud tertentu mulai dari rasa keingintahuan, coba-coba, *research*, tugas praktikum, kejahatan dan lain-lain (Sinambela, 2009).

Karena pentingnya menjaga keamanan jaringan *wireless*, maka diperlukan keamanan yang kuat. Untuk mengetahui seberapa kuat keamanan yang telah dibangun, maka dilakukan analisis yang nantinya hasil dari penelitian akan dijadikan kesimpulan dan saran bagi pengelolah jaringan *wireless* pada pemerintah kota prabumulih. *Wardriving* menjadi amcaman yang ditakuti oleh instansi yang menggunakan *wireless*, khususnya bagi pemerintah kota prabumulih yang menggunakan *wireless* sebagai penyedia internet.

2. METODOLOGIPENELITIAN

2.1. Metode Penelitian

Metode penelitian yang digunakan adalah metode penelitian tindakan (*action research*) adalah salah satu bentuk rancangan penelitian, dalam penelitian tindakan peneliti mendeskripsikan, menginterpretasi dan menjelaskan suatu situasi sosial pada waktu

yang bersamaan dengan melakukan perubahan atau intervensi dengan tujuan perbaikan atau partisipasi. *Action research* dalam pandangan tradisional adalah suatu kerangka penelitian pemecahan masalah, dimana terjadi kolaborasi antara peneliti dengan *client* dalam mencapai tujuan (Kurt Lewin,1973 disitasi Sulaksana,2004), sedangkan pendapat Davison, Martinsons & Kock (2004), menyebutkan penelitian tindakan, sebagai sebuah metode penelitian, didirikan atas asumsi bahwa teori dan praktik dapat secara tertutup diintegrasikan dengan pembelajaran dari hasil intervensi yang direncanakan setelah diagnosis yang rinci terhadap konteks masalahnya.

2.2. Metode Pengumpulan Data

Ada tiga tahapan yang harus dilakukan dalam proses pengumpulan data adalah sebagai berikut:

1. Metode Kepustakaan
   Metode ini digunakan untuk mengumpulkan data-data dan rumus-rumus yang diperlukan.
2. Wawancara
   Metode ini dilakukan dengan mengadakan tanya jawab (wawancara) secara langsung dengan pihak-pihak yang berkaitan dengan informasi.
3. Metode observasi
   Metode ini dilaksanakan dengan melakukan peninjauan langsung pada objek penelitian serta melakukan pencatatan mengenai hal-hal dan semua kejadian yang berhubungan dengan masalah yang diteliti. Observasi dilakukan di SMK Negeri 2 Palembang.

2.3 Metode Pengujian

Adapun Metode pengujian yang digunakan untuk penelitian ini adalah metode *Wardriving. Wardriving* adalah kegiatan seseorang yang melakukan kegiatan berkeliling ke berbagai ke tempat dalam usahanya mencari, mengekplorasi, bahkan mungkin juga mengekplotasi jaringan *wireless* yang ditemukannya. Kemudian orang yang melakukan kegiatan tersebut disebut sebagai *Wardriver*, dalam upanyanya itu dia melakukan pengumpulan data dan menganalisa sistem *Security*-nya (Zam, 2014). Tahapan dari metode *Wardriving* adalah :

a. Penguatan Sinyal

Untuk mendapatkan sinyal lebih kuat, peneliti akan menggunakan Wajan Bolic. Penggunaan Wajan Bolic agar sinyal dari jaringan wireless pada kantor pemerintah kota prabumulih dapat ditembuh dari jarak yang lebih jauh.

b. *Scaning*

Untuk melakukan Scaning, peneliti akan menggunakan *Tools* G-MoN yang dioperasikan di Android. *Software* ini akan memberikan informasi tentang *Channel*, MAC *address*, SSID, *Speed*, tipe Enkripsi, dari jaringan *wireless* yang akan di teliti yaitu jaringan *wireless* pada kantor pemkot prabumulih.

c. Pemetaan

Setelah dilakukan *Wardriving*, Informasi yang dihasilkan dari G-MoN akan diolah menggunakan Laptop sistem Operasi *Windows*. Titik-titik *Hotspot* yang sudah di *capture* menggunakan G-MoN akan disambungkan ke Google *Earth* sehingga hasil dari *Wardriving* dapat dipetakan.

d. *Cracking*

Setelah mendapatkan informasi berupa AP (*Access Point*), MAC *address (Media Access Control Address)*, Tipe Enkripsi dan BSSID (*Basic Service Set Identification)*, peneliti akan melakukan *Crack* untuk mendapatkan akses dari *wireless* tersebut sesuai dari Tipe keamanan. Peneliti akan menggunakan *software* CommView *for* Wifi versi 6 dan *Aircrack* jika tipe keamanan yang digunakan adalah WEP. Jika Tipe keamanan yang digunakan adalah WPA atau WPA2 peneliti akan menambahkan teknik *Brute Force Atack* sebagai usaha untuk mendapatkan akses internet pada jaringan wireless pemkot prabumulih.

2.4 *Scanning* dan Pemetaan

Pada fase ini, pemetaan dilakukan menggunakan Android Acer Z500. Scanning dilakukan mengelilingi gedung pemkot dengan kendaraan mobil. Seperti yang sudah dijelaskan sebelumnya, tindakan *Hacking/Craking* adalah suatu bentuk tindak kejahatan terkecuali telah mendapat izin resmi dari pihak yang terkait. Pada penelitian ini, peneliti sudah mendapat izin resmi dari pemkot prabumulih.

Scanning dimulai dari depan gedung pemkot, dilanjutkan dengan memutari gedung pemkot. Proses scanning dilakukan berulang kali untuk mendapatkan hasil yang lebih baik. Setelah selesai, proses *scanning* di *stop* dan hasil *scanning* di-*export* menjadi *file* berektensi KML yang dapat dibuka menggunakan *google earth.*

2.5. *Channel Capture*

Pase pertama dalam melakukan craking adalah *Channel capture*, *Software* yang digunakan peneliti adalah commview *for* wifi versi 7 yang dibuat oleh perusahaan Tamosoft. Peneliti akan menggunakan *single channel mode* agar mendapatkan *channel* yang lebih akurat karena *wireless* yang menjadi target adalah *wireless* yang disediakan oleh KOMINFO. Dengan mengklik tombol *capture* pada bagian kiri atas *software* commview *for* wifi maka proses *capture* akan mulai berjalan.

2.6. Injeksi Paket

Setelah memilih titik *hotspot* yang akan dijadikan target dengan mengklik dua kali pada nama dari *hotspot* tersebut, langkah selanjutnya adalah mengklik tab *packets.* Pada kolom *packets* dapat dilihat aktifitas jaringan wireless yang dipilih. Yang perlu dilakukan pada pase ini adalah memilih *protocol* yang berformat ENCR data.

Pada pase ini diperlukan *client* pada jaringan *wireless* target yang akan melakukan

login dengan mengetikan *password*, sehingga proses ini memakan waktu yang cukup lama. Tindakan itulah yang akan ditangkap oleh commview *for* wifi sehingga *password/keys* yang dimasukan oleh target dapat di tangkap (sadap). Untuk mempersiapkan hasil dari injeksi paket ialah dengan mengatur lokasi dan ukuran penyimpanan dengan mengklik tab *logging*.

2.7. *Concacenate Logs*

Setelah proses injeksi paket atau *send packets* selesai. Hasil yang didapat adalah *file* dengan ekstensi NCF. Format ini hanya bisa dibaca menggunakan *software* commview for wifi. Dari hasil yang didapat *Logs* yang telah dihasilkan dari proses injeksi paket akan digabungkan *(concacenate)*. Proses ini bertujuan agar *packets* yang bertebaran yang telah ditangkap digabungkan menjadi satu *file* saja. Pada *tab Logging* proses penggabungan *Logs* dilakukan dengan mengklik tombol *Concacenate Logs* dan selanjutnya menemukan lokasi penyimpanan yang telah diatur sebelumnya.

2.8. *Export Logs*

Dari hasil *Concacenate logs*, dihasilkan file yang berformat NCF. Ekstensi ini hanya bisa dibaca dengan menggunakan *software* commview for wifi. Pada proses *Export Logs* bertujuan untuk mengubah ekstensi dari *file* hasil *concacenate logs* (NCF) menjadi file berekstensi CAP. CAP adalah format *file* yang dapat dibaca dengan menggunakan *software Aircrack*.

2.9. *Handshake*

Handshake adalah aktifitas sebuah komputer terhadap *device* lainnya, seperti modem, *network servers*, *printers* dan lainnya. Pada kasus penelitian ini yang dimaksud *handshake* adalah aktifitas sebuah komputer dalam mengakses jaringan *wireless* yang menjadi target penelitian yaitu *wireless* kominfo Lt 1A. Untuk mengetahui apakah ada aktifitas *login wireless* target, peneliti menggunakan *software Aircrack* NG 1.2.

Dari informasi awal yang didapat pada saat melakukan pemetaan menggunakan G-mon diketahui keamanan yang digunakan pada jaringan *wireless* pemkot prabumulih adalah WPA. Untuk melakukan *crack* pada WPA diperlukan *Dictionary file* atau yang dapat diunduh di internet. Pada tampilan awal *aircrack* peneliti mengklik tombol WPA sesuai dengan tipe keamanan yang digunakan pada jaringan *wireless* pemkot prabumulih. Pada fase ini *file* berformat CAP yang sudah dihasilkan menggunakan commview *for* wifi pada proses sebelumnya dipanggil kembali *(load).* Peneliti akan mengklik tombol *Launch* untuk memulai *cracking*.

3. HASIL

3.1. Pemetaan G-Mon

Dari hasil *Scanning* menggunakan *Software* G-Mon yang dioperasikan menggunakan Android Acer Z500. G-Mon menghasilkan file yang berformat KML, file

ini dapat dibuka menggunakan Google Earth. Pada penelitian ini peneliti menggunakan laptop yang telah ter-*instal Google Earth*.. Berikut ini adalah hasil dari proses scanning yang telah dipetakan melalui *google earth.* Gambar 4.1 adalah hasil dari proses *scanning* yang dilakukan menggunakan *software* G-Mon yang dioperasikan menggunakan Android Acer Z500.

Titik-titik berwarna hijau, kuning, orange dan merah pada gambar 4.1 adalah titik *hotspot* yang tertangkap. Dari hasil yang diperoleh, dapat kita ketahui jumlah titik *hotspot* yang ada dan mengetahui beberapa informasi didalamnya. Dengan mengklik salah satu titik dapat mengetahui informasi berupa SSID, *Signal Strenght* (kekuatan sinyal), *Channel* dan juga tipe keamanan. Hasil dari pemetaan memudahkan peneliti untuk memilih titik *hotspot* mana yang akan dijadikan target untuk melakukan aksi *cracking* yang bertujuan mendapatkan *keys/password.*

Gambar 1. Google Earth

Pada gambar 1 adalah hasil pemetaan menggunakan software G-Mon, dapat dilihat ada beberapa titik *hotspot* yang berhasil di-*capture* menggunakan G-Mon. Warna pada titik *hotspot* tersebut adalah jenis keamanan yang digunakan. Titik yang berwarna merah adalah *hotspot* yang menggunakan keamanan WPA2, titik yang berwarna orange adalah *hotspot* yang menggunakan keamanan WPA, titik yang berwarna kuning adalah *hotspot* yang menggunakan keamanan WEP dan titik yang berwarna hijau adalah *hotspot* yang tidak menggunakan keamanan atau *Open.* Berikut adalah hasil pemetaan menggunakan G-Mon dalam bentuk tabel.

Tabel 1. Tabel pemetaan G-Mon

NO	SSID	Tipe keamanan	*Channel*
1	DPPKAD 01	WPA	1
2	DPPKAD 02	WPA	1
3	DPPKAD 04	WPA	1
4	DPPKAD 12	WPA	7
5	DPPKAD 22	WPA	7
6	DPPKAD 51	WPA	7
7	DPPKAD 52	WPA	7
8	DPPKAD 61	WPA	7
9	Kominfo Lt.1A	WPA	6
10	Kominfo Lt.1B	WPA	6
11	Kominfo Lt.3A	WPA	6
12	Kominfo Lt.5A	WPA	6
13	Kominfo Lt.7B	WPA	6
14	*HOTSPOT* SPEEDY 03	WPA	4
15	*HOTSPOT* SPEEDY 04	WPA2	4
16	PID PEMKOT-1	WPA2	3
17	DISHUB KOMINFO	WPA2	9
18	DINAS PU	WPA2	9
19	Groovia 5E48	WPA2	12
20	DINAS PERTANIAN	WPA2	6
21	INSTPEKTORAT 01	Open	1
22	Jaringan Bebas	WEP	5

Dari hasil pemetaan yang dilakukan menggunakan software G-Mon dapat dilihat jumlah titik *hotspot* yang berhasil ter-*capture*,

SSID, tipe keamanan dan juga *channel*. Pada saat melakukan pemetaan menggunakan software G-Mon peneliti juga mendapati titik *hotspot* diluar dari gedung pemkot, selain itu peneliti juga mendapati *hotspot* dengan *Hiden* SSID atau *hotspot* yang tidak menampilan SSID. Peneliti juga mendapati *Hotspot* dengan penggunaan berbayar. Berikut ini adalah *hotspot* yang dimaksud dalam bentuk tabel.

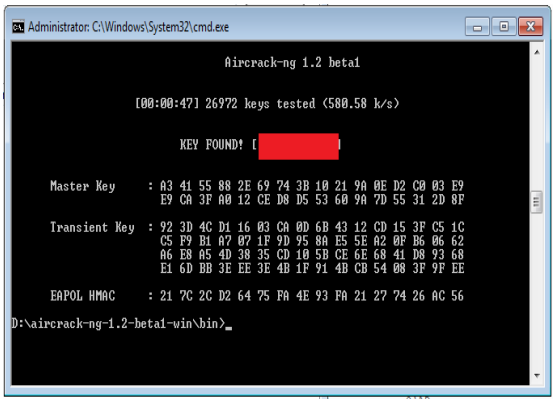
Tabel 2. Tabel Pemetaan G-Mon Lainnya

NO	SSID	Tipe keamanan	*Channel*
1	Wifiid	Open	3
2	Speedy Instanwifiid	Open	3
3	Speedy Instanwifiid	Open	9
4	*Wireless*Net	Open	5
5	RUMDIS KAPOLRES	WPA	2
6	Reskrim	WPA2	5
7	UNKNOWN	WPA2	2
8	UNKNOWN	WPA	2

Pada Tabel 2 adalah hasil pemetaan G-Mon yang didapati tanpa SSID, diluar dari gedung pemkot dan *hotspot* penggunaan yang berbayar. *Hotspot* Wifiid, Speedyinstanwifiid dan *Wireless*Net adalah *hotspot* dengan penggunaan berbayar, artinya untuk menggunakan *hotspot* tersebut harus melakukan pembayaran atau registrasi sebelumnya berupa tagihan operator seluler (pulsa). *Hotspot* RUMDIS KAPOLRES dan Reskrim adalah *hotspot* yang berada diluar gedung pemkot yang ikut ter-*capture* pada saat peneliti melakukan pemetaan menggunakan *software* G-Mon. *Hotspot* UNKNOWN adalah *hotspot* yang *Hiden* SSID atau *hotspot* yang tidak menampilkan SSID.

3.2. *Cracking Keys*

Berikut ini adalah hasil dari proses *cracking keys* terhadap *Hotspot* Kominfo Lt.1A yang dilakukan menggunakan *software* commview *for* wifi dan dilanjutkan dengan menggunakan *software* aircrack. Hasil *cracking* berupa Comand Prompt yang berisikan informasi *keys/password* target yang telah di-*crack* pada proses sebelumnya.

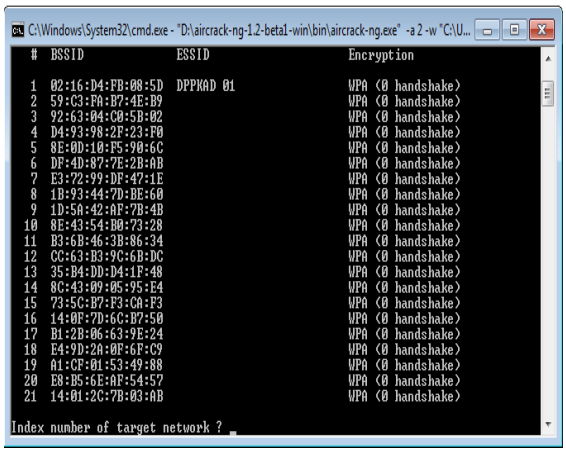


Gambar 2. *Keys/Password* Ditemukan

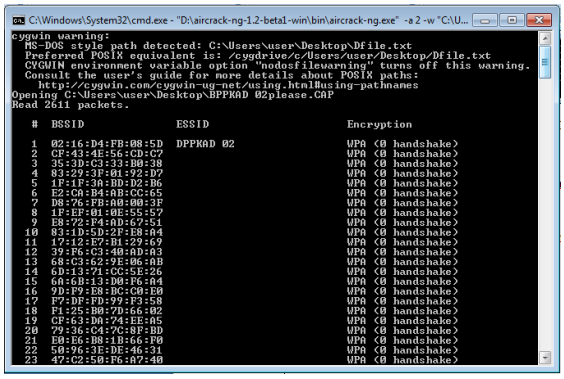
Gambar 2 adalah hasil dari proses *Cracking*. Terlihat pada *command prompt* tersebut tertulis "*KEY FOUND*" atau *password* ditemukan. *Keys/password* berhasil didapatkan setelah mencoba beberapa *dictionary file* atau kamus *password* yang telah diunduh dari berbagai sumber di internet. Peneliti juga mendapati *password* dari *hotspot* Kominfo Lt.1B, Kominfo Lt.3A, Kominfo Lt 5A, Kominfo LT 7B sama dengan password yang digunakan pada *hotspot* Kominfo Lt.1A. hal ini diketahui peneliti dengan login pada

hotspot tersebut menggunakan password yang sama dengan *hotspot* kominfo Lt.1A.

Peneliti sengaja tidak memperlihatkan *password* dikarenakan tidak mendapat izin dari pihak pemkot prabumulih. Hal ini sudah dimusyawarakan ketika peneliti berhasil mendapatkan *password* dari jaringan *wireless* pemkot. Setelah *password* berhasil ditemukan/diketahui oleh peneliti, peneliti dapat login dengan menggunakan password untuk mendapatkan akses internet pada *wireless* pemkot. Berikut ini adalah hasil percobaan *Cracking* pada *hotspot* DPPKAD 01 dan *hotspot* DPPKAD 02 .

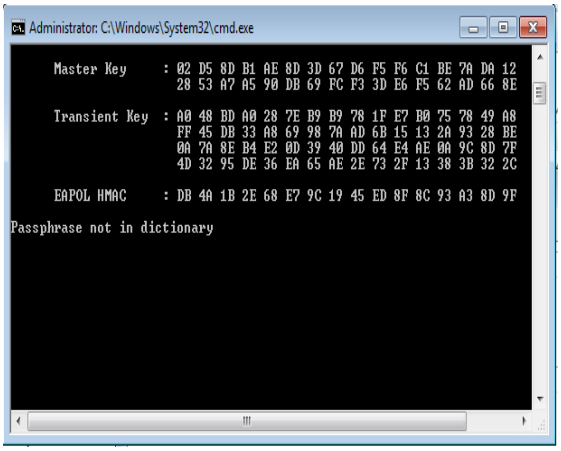


Gambar 3. Tidak menemukan *Handshake* DPPKAD 01



Gambar 4. Tidak menemukan *Handshake* DPPKAD 02

Gambar 3 dan 4 peneliti tidak menemukan *handshake* pada *hotspot* DPPKAD 01 dan DPPKAD 02. Terlihat pada bagian ”*Encryption”* tertulis <0 *handshake*> yang berarti tidak ada *handshake* . Hal ini terjadi karena tidak adanya *client* dari pengguna *hotspot* DPPKAD 01 dan DPPKAD 02 yang melakukan *login* dan mengetikan *password* selama proses injeksi paket sebelumnya yang dilakukan menggunakan *software* commview *for* wifi. Berikut ini hasil dari percobaan *Craking* pada *hotspot* DISHUB KOMINFO.



Gambar 5. *Key/Password* tidak ditemukan

Pada gambar 4.5, peneliti tidak berhasil mendapatkan *keys/password* pada *hotspot* DISHUB KOMINFO. Peneliti telah menggunakan beberapa *dictionary file* tetapi *keys/password* tetap tidak ditemukan. Hal ini berarti *password* yang digunakan pada *hotspot* DISHUB KOMINFO sudah kuat. Kemungkinan *password* yang digunakan pada *hotspot* DISHUB KOMINFO adalah berupa huruf besar, huruf kecil, angka dan simbol.

4. PEMBAHASAN

Dalam melakukan penelitian, peneliti mendapati beberapa kendala. Kendala yang dihadapi adalah seperti sulitnya mendapat posisi parkir mobil yang pas, baterai laptop habis, angin yang membuat sinyal tidak stabil dan juga *blue screen* (layar biru) atau laptop eror saat melakukan injeksi paket. Karena metode yang digunakan adalah *wardriving*, peneliti melakukan *cracking* didalam mobil, sehingga posisi parkir yang pas menunjang keberhasilan proses *cracking.* Proses *cracking* juga membutuhkan waktu yang cukup lama, energi baterai yang digunakan pada laptop terbatas sehingga proses *cracking* terkadang terhenti dikarenakan baterai pada laptop habis. Angin juga mempengaruhi sinyal, keberadaan peneliti pada luar ruangan dan titik *hotspot* yang tinggi membuat sinyal tidak stabil sehingga membuat proses cracking terganggu dan gagal. Disaat melakukan injeksi paket, peneliti sering kali mendapati *blue screen* atau bisa disebut laptop eror. Hal ini terjadi karena disaat melakukan injeksi paket dibutuhkan RAM laptop yang kuat.

Pada *Hotspot* Kominfo Lt.1A peneliti berhasil mendapatkan atau meng-*crack keys/password.* Setelah mendapatkan *password*, peneliti dapat mengakses jaringan *wireless* pada *hotspot* kominfo Lt.1A menggunakan *password* yang telah didapat dengan cara *login* seperti biasa. Peneliti juga mencoba login pada beberapa *hotspot* menggunakan *password* yang sama yaitu *hotspot* Kominfo Lt.1B, *hotspot* Kominfo Lt.3A, *hotspot* Kominfo Lt 5A dan *hotspot* Kominfo LT 7B. Peneliti berhasil *login* pada beberapa *hotspot* tersebut menggunakan password yang sama dengan yang *password* yang digunakan pada *hotspot* Kominfo Lt.1A.

Pada *Hotspot* DPPKAD 01 dan *Hotspot* DPPKAD 02 peneliti tidak berhasil melakukan *cracking* karena tidak ditemukannya *handshake* atau tidak adanya *client* yang melakukan *login* terhadap *hotspot* DPPKAD 01 dan *hotspot* DPKKAD 02 saat peneliti melakukan injeksi paket. Hal ini bisa disebabkan karena sedikitnya pengguna *hotspot* tersebut atau juga terbatasnya waktu peneliti saat melakukan injeksi paket sehingga belum sempat didapatkan *client* yang *login* dengan mengetikan *password* pada *hotspot* DPKKAD 01 dan *hotspot* DPPKAD 02.

Pada *Hotspot* DISHUB KOMINFO, peneliti mendapati *handshake* tetapi tidak bisa mendapatkan *keys/password.* Peneliti sudah mencoba beberapa *dictionary file* atau kamus *password* dan tetap tidak berhasil. Hal ini dikarenakan *password* yang digunakan pada *hotspot* DISHUB KOMINFO sudah kuat atau menggunakan *password* yang unik yaitu berupa huruf kecil, huruf besar, angka dan simbol. Berbeda dengan *hotspot* DISHUB KOMINFO, *hotspot* Kominfo Lt.1A tidak memiliki *password* yang kuat atau unik. *Keys/password* yang digunakan pada *hotspot* Kominfo Lt.1A adalah berupa huruf kecil yang berjumlah 8 karakter tanpa kombinasi huruf besar, angka atau simbol. Hal ini membuat *Hotspot* Kominfo Lt.1A cukup mudah untuk di-*Crack*. Pada beberapa *hotspot* lainnya yang

berada pada gedung pemkot prabumulih, peneliti tidak mendapati izin penuh sehingga penelitian hanya meneliti beberapa *hotspot* saja yang telah diberikan izin dari pihak pemkot.

Setelah dilakukan pengujian, peneliti dapat melakukan *craking* dan berhasil mendapatkan akses internet pada *Hotspot* Kominfo Lt.1A dan juga berhasil login pada beberapa *hotspot* yang menggunakan *password* yang sama dengan *password* yang digunakan pada *hotspot* Kominfo Lt.1A. Hal ini tentu berbahaya jika dilakukan oleh orang yang tidak bertanggung jawab. Seperti teknik *Snifing*, *client* yang tidak bertanggung jawab bisa saja melakukan *sniffing* untuk mendapatkan *password client* lain yang melakukan *login email*, *facebook, twiter* dan lainnya. Atau juga melakukan aksi pencurian data dengan memanfaatkan kelalaian pengguna lain yang sedang melakukan *file sharing*. Pada penelitian ini peneliti tidak diizinkan untuk melakukan aksi tambahan.

Seperti yang diketahui bahwa suatu jaringan *wireless* dapat dikatakan aman jika memenuhi prinsip dasar keamanan jaringan yaitu Kerahasiaan (*secrecy*), Integritas (*integrity*) dan ketersediaan (*availability*). Pada penelitian ini, peneliti berhasil mendapatkan *keys/password* dan berhasil login pada jaringan wireless pemkot prabumulih, artinya keamanan jaringan wireless pada pemkot prabumulih tidak memenuhi prinsip dasar keamanan jaringan pada point 3 yaitu ketersediaan (*availability*) yang tertulis bahwa suatu keamanan jaringan *wireless* dapat dikatakan aman jika diakses atau dimanfaatkan oleh pihak yang berhak. Dari hasil analisa yang dilakukan, peneliti dapat menyimpulkan bahwa jaringan *wireless* pada pemkot prabumulih tidak aman.

Agar keamanan jaringan *wireless* pada pemkot lebih optimal, perlunya menambahkan keamanan yang lebih kuat pada semua titik *hotspot* yang digunakan. Seperti menggunakan *password* yang rumit yaitu *password* dengan kombinasi huruf kecil, huruf besar, angka dan simbol. Atau dengan mengaktifkan MAC *Address Filtering* sehingga hanya perangkat dengan MAC *address* tertentu saja yang boleh mengakses kedalam jaringan *wireless* yang dikelolah. Untuk menghindari Injeksi paket saat seseorang melakukan *cracking* adalah dengan mengaktifkan mode *Connect Automatically* yaitu dengan men-centang bagian *Connect Automatically* pada saat melakukan *login* ke jaringan *wireless*. Cara tersebut dapat mencegah injeksi paket karena disaat seseorang melakukan injeksi paket yang dibutuhkan adalah *client* yang login kesebuah jaringan *wireless* dengan mengetikan password. Jika didapati PC yang menggunakan *software Deep Freeze*, sebaiknya *software* tersebut di-*uninstall* selanjutnya lakukan *login* dengan mengaktifkan mode *Connect Automatically*, lalu pasang kembali software *Deep Freeze*.

Pada saat melakukan Pemetaan dan *cracking*, peneliti tidak mendapati kecurigaan dari pihak pemkot prabumulih, artinya keamanan pada lahan parkir di kantor pemkot prabumulih kurang optimal. Sehingga

masyarakat umum dapat memasuki lahan parkir dengan mudah dan kegiatan yang dilakukan pada lahan parkir gedung pemkot tidak terpantau dengan baik. Hal ini membuat pelaku *wardriving* dapat dengan mudah melakukan *wardriving* pada pemkot prabumulih. Jika keamanan pada gedung pemkot dapat dioptimalkan, kegiatan *wardriving* dapat diminimalisir bahkan dicegah.

5. KESIMPULAN

Setelah dilakukan analisa terhadap keamanan jaringan *wireless* pada kantor pemerintah kota prabumulih dengan menggunakan metode *wardriving*, peneliti dapat menyimpulkan hasil dari penelitian sebagai berikut:

1. Jaringan *wireless* pada kantor pemerintah kota prabumulih tidak aman, karena masih ada titik hotspot yang bisa dilakukan *cracking* dan berhasil mendapatkan *password/keys*.
2. Pada *hotspot* Kominfo Lt.1A digunakan *password* yang ringan yaitu menggunakan huruf kecil tanpa kombinasi angka, huruf besar ataupun simbol.
3. *Password* yang digunakan pada *hotspot* Kominfo Lt.1B, Kominfo Lt.3A, Kominfo Lt 5A, Kominfo LT 7B sama dengan *password* yang digunakan pada *hotspot* Kominfo Lt.1A.
4. Kurangnya pengawasan terhadap lahan parkir gedung pemkot prabumulih.

DAFTAR RUJUKAN

Aditya Wahyu Setyawan, Gunawan Adi, Muhammad Ary Murti (2007). *Analisis system keamanan jaringan wirelesslan dengan menggunakan metode wardriving*. Dari:http://repository.telkomuniversity.ac.id/pustaka/files/90474/resume/analisis-sistem-keamanan-jaringan-wirelesslan-dengan-menggunakan-metode-wardriving.pdf diakses pada desember 2015.

Ch.sai priya, Syed umar, T sirisha (2006). *The impact of wardriving on wireless networks*. Dari:http://ijcset.net/docs/volumes/volume3issue6/ijcset2013030605.pdf diakes pada desember 2015.

Efvy Zamidra Zam (2014) *Wireless Hacking*

Hira sathu (2006). *Wardriving dilemmas.* Dari: *citrenz.ac.nz/conferences/2006/papers/237.pdf diakses pada desember 2015.*

Gondohanindijo, *Sistem Keamanan Jaringan NIRKABEL* (2012) dari https://www.google.co.id/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjEm43NnffKAhVGZCYKHSU7CXQQFggkMAE&url=http%3A%2F%2Fwww.unaki.ac.id%2Fejournal%2Findex.php%2Fjurnal-informatika%2Farticle%2Fdownload%2F20%2F19&usg=AFQjCNETOKN

fyyN2NeY9d7_tD9eWzAuJZQ&bvm=bv.114195076,d.eWE *diakses pada desember 2015*

https://en.wikipedia.org/wiki/Wardriving *diakses pada desember 2015.*

http://library.binus.ac.id/eColls/eThesisdoc/Bab2HTML/2013101345IFBab2001/page12.html diakses pada desember 2015

https://id.wikipedia.org/wiki/Wired_Equivalent_Privacy diakses pada desember 2015.

http://sir.stikom.edu/273/6/BAB%20III.pdf diakses pada September 2015.

http://www.adalahcara.com/2013/05/pengertian-kelas-ip-address-adalah.html diakses pada september 2015.

http://adefachreza.blogspot.com/2013/09/pengertian-access-point-dan-fungsinya.html diakses pada september 2015.

Kern, Benjamin D (2005). *Whacking, joyriding and war-driving: roaming use of wi-fi and the law*. Dari: http://digitalcommons.law.scu.edu/chtli/vol21/iss1/3 diakses pada septermber 2015.

Nugroho (2012). *Analisa Keamanan Jaringanwireless Local Area Network Dengan Access Point Tp-Link Wa500g.* Dari http://eprints.ums.ac.id/20254/20/Naskah_Agung_Nugroho_L200080023.pdf Diakses pada september 2015.

Reza jalaluddin Al-haroh(2012). *Wardriving dan testing penetrasi wi-fi lanjut di wilayah kota Yogyakarta,* dari: http://repository.amikom.ac.id/files/publikasi_08.11.2153.pdf diakses pada desember 2015.

Rushadi (2009). *Konsep Keamanan Jaringan Komputer dengan Infrastruktur Demilitarized Zone.* Dari http://www.academia.edu/11938528/Konsep_Keamanan_Jaringan_Komputer_dengan_Infrastruktur_Demilitarized_Zone diakses pada september 2015.

Securekomodo.com/hacking-wpa-wpa2-encrypted-networks/ diakses pada September 2015.

Stiawan (2008), *Wireless Fundamental, Instalation & Implemetations.* Dari *:* http://*amikom.ac.id/research/index.php/KIM/article/viewFile/3160/1494 diakses pada desember 2015.*

Vyctoria (2014) *Tips & Trik Jaringan Wireless*