

**WARDRIVING DAN TESTING PENETRASI WI-FI LANJUT DI
WILAYAH KOTA YOGYAKARTA**

SKRIPSI



disusun oleh

Reza Jalaluddin Al-Haroh

08.11.2153

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER**

AMIKOM

YOGYAKARTA

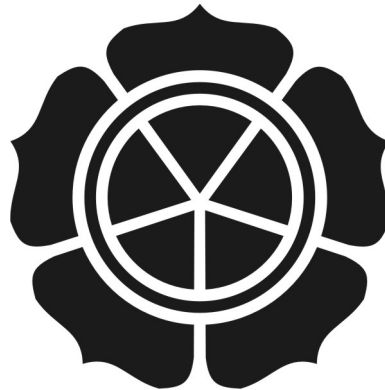
2012

WARDRIVING DAN TESTING PENETRASI WI-FI LANJUT DI

WILAYAH KOTA YOGYAKARTA

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



disusun oleh

Reza Jalaluddin Al-Haroh

08.11.2153

JURUSAN TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

AMIKOM

YOGYAKARTA

2012

PERSETUJUAN

SKRIPSI

**Wardriving dan Testing Penetrasi Wi-Fi Lanjut
di Wilayah Kota Yogyakarta**

yang dipersiapkan dan disusun oleh

Reza Jalaluddin Al-Haroh

08.11.2153

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 12 Desember 2011

Dosen Pembimbing,



Sudarmawan, MT
NIK. 190302035

PENGESAHAN

SKRIPSI

**Wardriving dan Testing Penetrasi Wi-Fi Lanjut
di Wilayah Kota Yogyakarta**

yang dipersiapkan dan disusun oleh

Reza Jalaluddin Al-Haroh

08.11.2153

telah dipertahankan di depan Dewan Penguji
pada tanggal 16 Juni 2012

Susunan Dewan Penguji

Nama Penguji

Krisnawati, S.Si, M.T
NIK. 190302038

Kusrini, Dr., M.Kom
NIK. 190302106

Sudarmawan, M.T
NIK. 190302035

Tanda Tangan







Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 10 Juli 2012

KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001



PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 25 Juni 2012

Reza Jalaluddin Al-Haroh
08.11.2153

MOTTO

"What you can do, or dream you can do, begin it!

Boldness has genius, power and magic in it."

-goethe-

"Champions aren't made in the gyms. Champions are made from something they have deep inside them - a desire, a dream, a vision."

-Muhammad Ali-

"You might try to restrict information, but technology enables us to stand as equals!."

- byteskrew-



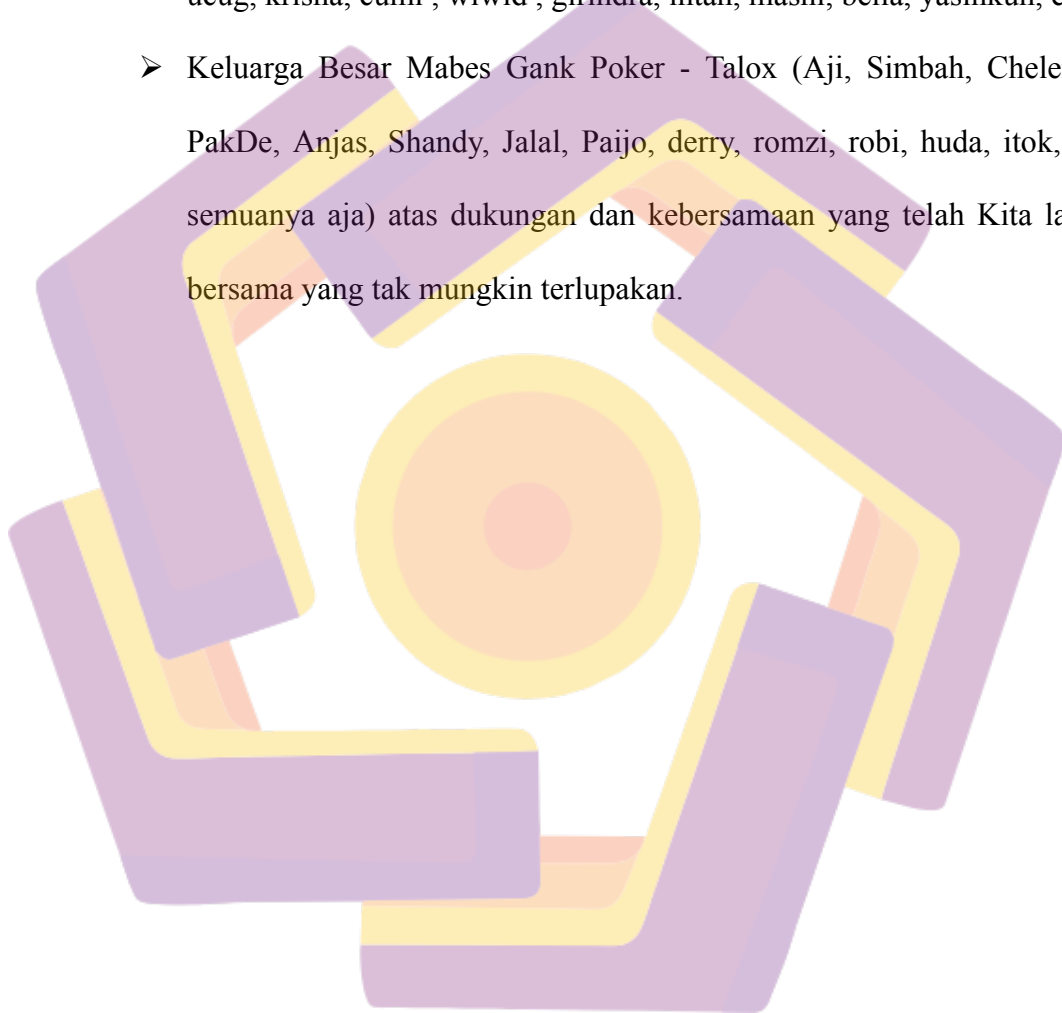
PERSEMBAHAN

Alhamdulillah akhirnya selesai juga setelah beberapa bulan berjuang. Skripsi ini bukanlah sesuatu yang terbaik, namun saya selaku penulis mempersembahkan skripsi ini khusus kepada :

- Allah SWT yang telah memberikan beribu anugerah terutama anugerah iman dan islam serta kesehatan sehingga skripsi ini dapat terselesaikan dengan baik.
- Nabi Muhammad SAW. Engkaulah yang membimbing kami di jalan yang benar.
- Ayah Hakiki mahfuzh, Ibu rahmatun, dan Adiku Fachri imaduddin al-haroh terima kasih atas kasih sayang selama ini yang tidak henti – hentinya memberikan doa dan dukungan moril maupun material dalam setiap langkahku serta didikan yang setiap saat selalu diberikan tanpa mengenal lelah.
- Sudarmawan, M.T selaku dosen pembimbing yang telah banyak memberikan pengarahan bagi penulis dalam pembuatan skripsi.
- Ultraman leader in the land of lights , Habieb ibnu jati, Newin Ananta see you on top guys we will make the world better.
- kecoak elektronik stuff, cyberheb(rasyid syahputra) ,phoenix(atik pilihanto), scut (betha morison), logcode (allesio ammario),

primadonal , etc. I know some day i will go abroad, and make you proud.

- Smada 08 : Dadid, yayan, risang, adam, hedar, asep, dici, maridjo, sogie, wuri, septian, hendi , danang, udin, vidya, ajoe, bekti, rani, raras, ucug, krisna, cumi , wiwid , girindra, intan, mashi, bella, yasinkun, etc.
- Keluarga Besar Mabes Gank Poker - Talox (Aji, Simbah, Chelenk, PakDe, Anjas, Shandy, Jalal, Paijo, derry, romzi, robi, huda, itok, n semuanya aja) atas dukungan dan kebersamaan yang telah Kita lalui bersama yang tak mungkin terlupakan.



KATA PENGANTAR


Alhamdulillah puji syukur penulis panjatkan kehadirat Allah SWT yang senantiasa melimpahkan rahmat dan anugerah kepada setiap hamba-hambanya yang beriman dan berikhtiar. Shalawat serta salam juga tidak lupa penulis kirimkan kepada junjungan kita Nabi Besar Muhammad SAW yang telah memberikan teladan mulia dalam menuntun umatnya.

Skripsi ini disusun sebagai salah satu syarat kelulusan bagi setiap mahasiswa STMIK “AMIKOM”. Selain itu juga merupakan suatu bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang program Strata-1 dan untuk memperoleh gelar Sarjana Komputer.

Dengan selesainya skripsi ini, maka penulis tidak lupa mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, M.M selaku Ketua STMIK “AMIKOM” Yogyakarta.
2. Bapak Sudarmawan, M.T selaku Ketua Jurusan Teknik Informatika STMIK “AMIKOM” Yogyakarta sekaligus pembimbing yang telah banyak memberikan pengarahan bagi penulis dalam pembuatan skripsi.
3. Bapak dan Ibu dosen STMIK “AMIKOM” Yogyakarta yang telah banyak memerikan ilmunya selama penulis kuliah.
4. Semua pihak yang telah membantu baik dukungan moril maupun materiil, pikiran, dan tenaga dalam penyelesaian skripsi ini.

Penulis tentunya menyadari bahwa pemuatan skripsi ini masih banyak sekali kekurangan-kekurangan dan kelemahan-kelemahannya. Oleh karena itu penulis berharap kepada semua pihak agar dapat menyampaikan kritik dan saran yang membangun untuk menambah kesempurnaan skripsi ini. Namun penulis tetap berharap skripsi ini akan bermanfaat bagi semua pihak yang membacanya.



Yogyakarta, 25 Juni 2012

Penulis

Reza jalaluddin Al-Haroh

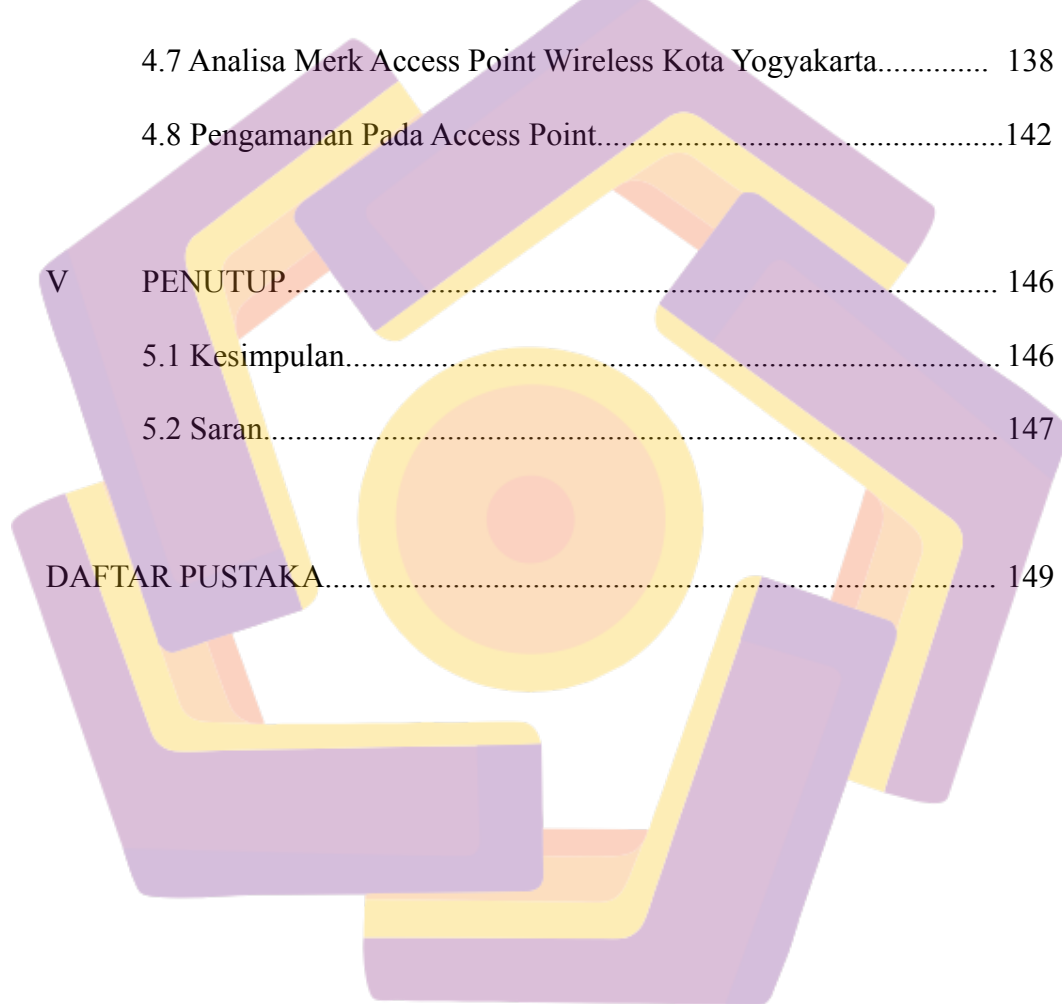
DAFTAR ISI

LEMBAR PERSETUJUAN.....	i
LEMBAR PENGESAHAN.....	ii
HALAMAN PERNYATAAN.....	iii
HALAMAN MOTTO.....	iv
HALAMAN PERSEMBAHAN.....	v
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xiv
DAFTAR TABEL.....	xix
INTISARI.....	xx
ABSTRACT.....	xxi
I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Perumusan Masalah.....	2
1.3 Batasan Masalah.....	2
1.4 Maksud dan Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Metode Pengumpulan Data.....	4
1.7 Sistematika Penulisan.....	5
II LANDASAN TEORI.....	7
2.1 Definisi Wireless dan Sejarahnya.....	7

2.2 Standar Jaringan Wireless	10
2.3 Komponen WLAN.....	15
2.3.1 Access Point (AP).....	15
2.3.2 Extension Point.....	18
2.3.3 Antena.....	19
2.3.4 Wireless LAN Card.....	22
2.3.5 Kelebihan dan Kelemahan implementasi WLAN.....	22
2.4 Topologi Jaringan Nirkabel.....	24
2.5 Mekanisme CSMA/CA.....	30
2.6 Definisi Wardriving.....	32
2.7 Sejarah Wardriving.....	33
2.8 Legalisasi Wardriving.....	34
2.9 Defini Penetration Testing.....	35
2.10 Sejarah Keamanan Wireless.....	36
2.11 Penyerangan Jaringan Wireless.....	38
2.11.1 Berbagai Jenis Serangan terhadap WLAN.....	38
2.11.2 Logical Attack dengan teknik mitigasi.....	38
2.11.2.1 Spoofing Mac Address.....	40
2.11.2.2 Serangan Denial of Service.....	40
2.11.2.3 Serangan Man in the Middle.....	41
2.11.2.4 Default Access Point Configuration.....	43
2.11.2.5 Serangan Reconnaissance.....	44
2.11.2.6 Conversation Sniffing.....	44

2.11.2.7 Serangan Dynamic Host Configuration Protocol....	45
2.11.3 Physical Attack dengan teknik mitigasi.....	46
2.11.3.1 Rogue Access Point.....	46
2.11.3.2 Physical Placement of Access Points.....	47
2.11.3.3 Access Point Coverage.....	47
2.11.3.4 Serangan Spam.....	47
2.12 Mekanisme Keamanan Wireless.....	48
2.12.1 Keamanan Wireless dengan metode WEP.....	48
2.12.2 Keamanan Wireless dengan metode WPA.....	49
2.12.3 WPA-PSK.....	50
2.12.4 WPA2.....	51
2.12.5 Kelebihan dan Kelemahan WEP dan WPA.....	51
III METODOLOGI PENELITIAN.....	53
3.1 Variable Penelitian.....	53
3.2 Persiapan dalam Wardriving.....	53
3.2.1 Area Kota Yogyakarta.....	53
3.3 Peralatan yang dibutuhkan untuk melakukan wardriving.....	56
3.3.1 Wardriving Menggunakan Mobil.....	56
3.3.2 Wardriving menggunakan Smartphone.....	59
3.3.3 Pembahasan khusus mengenai Wigle.....	59
3.4 Pemilihan Network Chipset.....	61
3.5 Pemilihan Antena.....	63

3.6	Pemilihan Sistem Operasi.....	65
3.7	Langkah - Langkah Wardriving.....	65
3.7.1	Wardriving pada sistem Operasi Macintosh.....	65
3.7.2	Wardriving pada sistem operasi Linux.....	68
3.7.3	Wardriving Menggunakan Smartphone Android.....	74
3.7.4	Tips Meningkatkan Tx Power Pada Chipset tertentu...	76
3.8	Pemetaan dalam Wardriving.....	78
3.9	Pembuktian konsep Wireless Penetration Testing.....	83
3.9.1	MAC Address Spoofing.....	83
3.9.2	Serangan Denial of Service.....	88
3.9.3	Serangan Man in the Middle.....	90
3.9.4	Default Access Point Configuration.....	92
3.9.5	Serangan Reconnaissance.....	96
3.9.6	Conversation Sniffing.....	99
3.9.7	Rogue Access points.....	101
3.9.8	Physical Placement of Access Point.....	105
3.9.9	Serangan Spam.....	106
3.9.10	WEP Cracking.....	108
3.9.11	WPA/WPA2 Cracking.....	114
3.9.12	WPS Cracking.....	118
IV	HASIL DAN PEMBAHASAN.....	120
4.1	Analisa Pemetaan pada Wardriving.....	120



4.2 Analisa Enkripsi Wireless Kota Yogyakarta.....	125
4.3 Analisa default SSID Wireless Kota Yogyakarta.....	127
4.4 Analisa Channel Wireless Kota Yogyakarta.....	130
4.5 Analisa Interferensi Channel Wifi Kota Yogyakarta.....	132
4.6 Pembuktian Interferensi Channel.....	133
4.7 Analisa Merk Access Point Wireless Kota Yogyakarta.....	138
4.8 Pengamanan Pada Access Point.....	142
V PENUTUP.....	146
5.1 Kesimpulan.....	146
5.2 Saran.....	147
DAFTAR PUSTAKA.....	149

DAFTAR GAMBAR

Gambar 2.1	Interference Channel Pada Wireless.....	14
Gambar 2.2	Access Point dari produk Linksys, Symaster, Dlink.....	15
Gambar 2.3	Jaringan Wireless Bridge.....	17
Gambar 2.4	Jaringan Wireless Client Mode.....	18
Gambar 2.5	Jaringan Menggunakan Extension Point.....	19
Gambar 2.6	Antena Omni Directional.....	20
Gambar 2.7	Jangkuan Area Antena Omnidirectional.....	21
Gambar 2.8	Jangkuan antena directional.....	21
Gambar 2.9	Wireless LAN Card.....	22
Gambar 2.10	Mode Ad-Hoc.....	25
Gambar 2.11	Mode Infrastructure.....	26
Gambar 2.12	Mode Half Duplex.....	27
Gambar 2.13	BSS.....	28
Gambar 2.14	EBSS.....	29
Gambar 2.15	Penggunaan root AP.....	30
Gambar 2.16	Spoofing MAC Address.....	40
Gambar 3.1	Peta Kota Yogyakarta.....	53
Gambar 3.2	Hardware Wardriving yang digunakan penulis.....	56
Gambar 3.3	Letak Perangkat Wardriving Pada Mobil.....	57
Gambar 3.4	Letak Antena Pada Mobil.....	58
Gambar 3.5	General Stat Wardriving pada Webseite Wigle.....	60

Gambar 3.6	Keadaan Peta Wardriving Seluruh Dunia.....	61
Gambar 3.7	Tampilan dari GPS over BT dan Kismac Preferences.....	65
Gambar 3.8	Tampilan dari Kismac Preferences Driver.....	67
Gambar 3.9	Tampilan Kismac pada waktu proses.....	68
Gambar 3.10	Tampilan dari BlueNMEA.....	69
Gambar 3.11	Pengecekan terhadap service rfcomm0.....	70
Gambar 3.12	Tampilan dari gpsd beserta contoh output.....	70
Gambar 3.13	Keterangan dari gpsd.....	71
Gambar 3.14	Output dari lsub dan airmon-ng.....	72
Gambar 3.15	Tampilan Kismet saat melakukan wardriving.....	73
Gambar 3.16	Tampilan dari GPS Kismet.....	74
Gambar 3.17	Tampilan dari Wigle Wireless Wardriving.....	75
Gambar 3.18	Tampilan Konversi dBm ke mW.....	76
Gambar 3.19	Perubahan Tx-Power dengan iwconfig.....	77
Gambar 3.20	Export ke google earth KML pada Kismac.....	78
Gambar 3.21	Hasil dari Kismac pada Google Earth.....	79
Gambar 3.22	Giskismet pada sistem operasi linux.....	80
Gambar 3.23	Hasil dari giskismet pada Google Earth.....	81
Gambar 3.24	Hasil dari Wigle Wifi Wardriving.....	82
Gambar 3.25	Penerapan Mac Address Filtering pada Access Point.....	83
Gambar 3.26	Tampilan airodump-ng pada mesin Attacker.....	84
Gambar 3.27	Gagal Koneksi ke SSID Mahfuzh.....	85
Gambar 3.28	Merubah Mac Address dengan Macchanger.....	86

Gambar 3.29	Device List AP sebelum Spoofing.....	87
Gambar 3.30	Device List AP setelah Spoofing.....	87
Gambar 3.31	Proses Denial of Service.....	88
Gambar 3.32	Tampilan Request Time Out Pada User.....	89
Gambar 3.33	Tampilan dari YAMAS.....	90
Gambar 3.34	Arpspoof dan Proses Capture Password.....	91
Gambar 3.35	Hasil sniffing username dan password.....	92
Gambar 3.36	Generate IP address Class C.....	93
Gambar 3.37	Tampilan THC-Hydra.....	94
Gambar 3.38	Hasil dari bruteforce dengan Password Default.....	95
Gambar 3.39	Nmap melakukan Scanning Port.....	96
Gambar 3.40	Nmap melakukan scanning service pada port terbuka.....	97
Gambar 3.41	Nmap melakukan scanning sistem operasi.....	98
Gambar 3.42	Tampilan tracroute berupa grafik dari Nmap.....	99
Gambar 3.43	Http packet pada saat melakukan sniffing.....	100
Gambar 3.44	Image yang direkam saat melakukan sniffing.....	100
Gambar 3.45	Ilustrasi Rogue Access Point.....	101
Gambar 3.46	Tampilan dari easy-creds.....	102
Gambar 3.47	IP Config pada User terkoneksi ke Rogue Access Point.....	103
Gambar 3.48	Proses Sniffing pada Rogue Access Point.....	104
Gambar 3.49	Tampilan Belakang Sebuah Access Point.....	105
Gambar 3.50	Tampilan mdk3 Spamming SSID.....	106
Gambar 3.51	Tampilan dari inSSIDer menscan banyaknya spam SSID.....	107

Gambar 3.52	Spamming client yang terkoneksi ke sebuah Access Point...	108
Gambar 3.53	Setting WEP pada Access Point.....	109
Gambar 3.54	Tampilan Airodump.....	109
Gambar 3.55	Airodump-ng pada Channel 1.....	110
Gambar 3.56	Proses deauthentication dengan aireplay-ng.....	111
Gambar 3.57	Banyaknya Packet Data yang terkumpul.....	111
Gambar 3.58	Proses WEP cracking.....	112
Gambar 3.59	Proses deencryption dengan airdecap-ng.....	113
Gambar 3.60	Proses analisa paket dengan tshark.....	113
Gambar 3.61	Setting WPA/WPA2 pada Access Point.....	114
Gambar 3.62	Airodump-ng pada channel 1.....	115
Gambar 3.63	Proses deauthentication dengan aireplay-ng.....	115
Gambar 3.64	WPA Handshake Found.....	116
Gambar 3.65	Proses WPA/WPA2 Cracking.....	116
Gambar 3.66	Proses deencryption dengan airdecap-ng.....	117
Gambar 3.67	Proses analisa paket dengan tshark.....	117
Gambar 3.68	Tampilan Airodump-ng.....	118
Gambar 3.69	Wash untuk mengetahui Access Point WPS.....	119
Gambar 3.70	Proses cracking WPS dengan Reaver.....	119
Gambar 4.1	Peta Wilayah Kota Yogyakarta.....	120
Gambar 4.2	Hasil Wardriving Wilayah Kota Yogyakarta.....	121
Gambar 4.3	Peta Open Wireless Wilayah Kota Yogyakarta.....	122
Gambar 4.4	Peta WEP Wireless Wilayah Koya Yogyakarta.....	123

Gambar 4.5	Peta WPA/WPA2 Wireless Wilayah Kota Yogyakarta.....	124
Gambar 4.6	Grafik Enkripsi Wifi Kota Yogyakarta.....	126
Gambar 4.7	Grafik default SSID dan Non Default SSID.....	128
Gambar 4.8	Default SSID Wifi Kota Yogyakarta.....	129
Gambar 4.9	Channel Wifi Kota Yogyakarta.....	131
Gambar 4.10	Interferensi Channel Wifi Kota Yogyakarta.....	133
Gambar 4.11	Time Graph dari inSSIDer.....	134
Gambar 4.12	Tampilan dari inSSIDER tidak terjadi Interferensi.....	134
Gambar 4.13	Tampilan dari Kismac tidak terjadi interferensi.....	135
Gambar 4.14	Tampilan Kismac terjadi Interferensi pada CHannel 11.....	136
Gambar 4.15	Tampilan Kismac terjadi Interferensi pada channel 11.....	136
Gambar 4.16	Tampilan inSSIDER terjadi interferensi Channel.....	137
Gambar 4.17	Time Graph pada inSSIDER terjadi Interferensi.....	137
Gambar 4.18	Merk Access Point Wifi Kota Yogyakarta.....	139

DAFTAR TABEL

Tabel 2.1	Channel dan Frekuensi Pada wireless.....	12
Tabel 2.2	Kelebihan dan kelemahan wireless dan LAN.....	22
Tabel 3.1	Data Kota Yogyakarta.....	54
Tabel 3.2	Daftar Merk Wireless Card beserta Chipset.....	62
Tabel 3.3	Daftar keterangan Symbol pada Output giskismet.....	82
Tabel 4.1	Enkripsi Wireless Kota Yogyakarta.....	125
Tabel 4.2	Default SSID dan Non Default SSID.....	127
Tabel 4.3	Default SSID Wifi Kota Yogyakarta.....	128
Tabel 4.4	List default Password.....	130
Tabel 4.5	Channel Wifi Kota Yogyakarta.....	130
Tabel 4.6	Interferensi Channel Wifi Kota Yogyakarta.....	132
Tabel 4.7	Pembuktian Interferensi Channel.....	135
Tabel 4.8	Pembuktian Interferensi Channel.....	138
Tabel 4.9	Merk Access Point Wifi Kota Yogyakarta.....	139
Tabel 4.10	Merk Access Point dan Serinya yang vulnerable WPS.....	140

INTISARI

Jaringan Wireless merupakan jargon teknologi yang paling berkembang saat ini, dan bisa di temui hampir diseluruh tempat baik itu tempat umum seperti cafe, kampus, supermarket, ataupun kawasan perumahan. Dengan mudahnya user melakukan sebuah koneksi ke internet dengan bantuan jaringan wireless tanpa memerlukan media kabel dikarenakan media jaringan di pancarkan melalui frekuensi radio.

Pemanfaatan jaringan komputer pada tempat-tempat publik ini, terkadang memang memberikan daya tarik tersendiri, terutama layanan nirkabel gratis (free hotspot). Jaringan nirkabel (wireless) yang bersifat broadcast membuat komunikasi data yang terjadi cenderung tidak aman, dan memang pengguna pada umumnya menyampingkan issue security pada IEEE 802.11 sehingga banyak intruders yang memfokuskan serangannya pada protokol satu ini. Sebut saja wardriving ataupun Cracking WPA/WEP/WPA2, MitM (Man in the Middle Attack) , bahkan membuat dummy Access Point yang digabung dengan client-side exploit dan MiTM pada protokol https.

Maka dari itulah di dalam skripsi ini akan membahas analisa tentang keadaan wireless di daerah kota yogyakarta baik itu dari segi pemetaan access point sehingga dapat dilakukan analisa tentang keamanan access point, channel yang digunakan, interfrensi channel , merk access point dan penjelasan tentang metode ataupun cara yang digunakan oleh intruder beserta cara untuk meminimalisir serangan tersebut.

Kata Kunci : wireless, wardriving, security, hacking, yogyakarta

ABSTRACT

Wireless network technology is the most currently developments, and can be encountered in nearly all public places like cafes, colleges, supermarkets, or residential areas. User easily make a connection to the internet by aid wireless networks without requiring cable because data be broadcast through radio frequency.

Use of computer networks in public places, sometimes it gives a special attraction, especially the free wireless service (free hotspot). Wireless network (wireless) that are broadcast to the data communications that occur tend to be not safe, and users are generally ignore security issues in IEEE 802.11 so that many Intruders focuses its attacks on the protocol on this one. Call it wardriving or Cracking WPA/WEP/WPA2, MitM (Man in the Middle Attack), and even make a dummy Access Point combined with client-side exploits and MITM on https protocol.

That is why in this paper will discuss the analysis of the circumstances of wireless in the Yogyakarta city, both in terms of mapping access point to allow for analysis of the access point security, the channel used, channel interference, brand access point and an explanation of the method or manner used by the intruder and instructions on how to minimize such attacks.

Keyword: *wireless, wardriving, security, hacking, yogyakarta*