

**ANALISIS PERFORMA SISTEM JARINGAN HOTSPOT
PT TELKOM NGAWI**

SKRIPSI



disusun oleh.

Ifan Candra Kusuma

10.11.4433

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2014**

**ANALISIS PERFORMA SISTEM JARINGAN HOTSPOT
PT TELKOM NGAWI**

SKRIPSI

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



disusun oleh:

Ifan Candra Kusuma

10.11.4433

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2014**

PERSETUJUAN

SKRIPSI

**ANALISIS PERFORMA SISTEM JARINGAN HOTSPOT
PT TELKOM NGAWI**

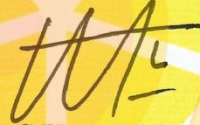
yang dipersiapkan dan disusun oleh

Ifan Candra Kusuma

10.11.4433

telah disetujui oleh dosen pembimbing skripsi
pada tanggal 10 desember 2014

Dosen pembimbing



Kusnawi, S.Kom, M.Eng
NIK. 190302112

PENGESAHAN
SKRIPSI
ANALISIS PERFORMA SISTEM JARINGAN HOTSPOT
PT TELKOM NGAWI

Yang disusun oleh
Ifan Candra Kusuma
10.11.4433

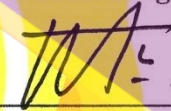
telah dipertahankan di depan Dewan Penguji
pada tanggal 5 desember 2014

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Kusnawi, S.Kom, M.Eng.
NIK. 190302112



Krisnawati, S.Si, MT.
NIK. 190302038




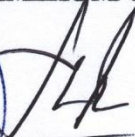
Sudarmawan, MT.
NIK. 190302035



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 12 Desember 2014

KEFUA SYM IK 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, 10 Desember 2014



Ifan Candra Kusuma
10.11.4433

MOTTO

- Silent is gold, but silent can give accidents speaking well and right is must better.
- Don't put until tomorrow what can you do today.
- One who says I don't know and learns is better than one who knows and puff himself up (Arabic proverb)
- Take time to quite, it is opportunity to seek god
- Bukti nyata adalah kepercayaan abadi
- Ready, willing and fully enabled! ~ Tinker
- Let weakness become strength! ~ Ember Spirit

PERSEMBAHAN

1. Allah SWT serta Nabi Muhammad SAW yang telah memberikan rahmat, karunia dan tuntunan sehingga saya diberi kelancaran dalam mencari ilmu dan menyelesaikan pendidikan S1 saya.
2. Keluarga besar tercinta, khususnya ayah dan ibu yang telah bekerja keras membanting tulang demi memberikan pendidikan yang tinggi kepada penulis, serta memberikan terus menerus dukungannya sehingga terselesaikannya skripsi ini.
3. Teman – teman seperjuangan yang ikut serta memberikan semangat dan motifasi, terimakasih untuk Joko, Agus, Palu, Icmi, Badrus, Rais.
4. Teman yang selalu ada di game, Shigit, Rekian, khirsna, Igo, Ryan, Titut.
5. Titis, Febri, Rani, Putri yang selalu ada dan selalu bersama.
6. Tidak lupa untuk kucingku Beda, setiap detik selalu menemaniku mengerjakan skripsi ini bahkan disaat susah senang dan sakit.

KATA PENGANTAR

Alhamdulillah, puji dan syukur kita panjatkan atas kehadiran Allah SWT yang telah memberikan rahmat dan hidayahnya sehingga penulis dapat menyelesaikan skripsi yang berjudul Analisis Performa Sistem Jaringan Hotspot PT. Telkom Ngawi. Shalawat serta salam tidak lupa kita tujukan kepada nabi Muhammad SAW, keluarga dan para sahabatnya, yang telah membawa kita dari jaman kegelapan sampai jaman yang terang benderang seperti yang kita rasakan saat ini.

Skripsi ini disusun bertujuan untuk memenuhi salah satu syarat kelulusan perguruan tinggi program studi Strata- 1 Teknik Informatika di Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.

Dengan selesainya skripsi ini, penulis tidak lupa mengucapkan terimakasih kepada:

1. Bapak Prof. Dr. M. Suyanto, M.M selaku ketua STMIK AMIKOM Yogyakarta.
2. Bapak Sudarmawan, MT selaku ketua jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
3. Bapak Kusnawi, S.Kom, M.Eng. selaku dosen pembimbing skripsi yang telah banyak membimbing penulis dalam menyelesaikan skripsi ini.
4. Bapak Agus Siswanto selaku Manager Kandatel Telkom Ngawi yang telah memberikan izin untuk melakukan penelitian ini.

5. Bapak dan ibu Dosen serta seluruh Staf dan Karyawan/ Karyawati STMIK AMIKOM Yogyakarta yang telah banyak memberikan ilmunya selama penulis mengikuti perkuliahan.
6. keluarga besar tercinta yang selalu memberikan dukungan dan doanya untuk terselesaikanya skripsi ini

penulis mengharpkan kritik dan saran yang membangun guna menyempurnakan skripsi ini sehingga dapat lebih bermanfaat bagi para pembaca.

Akhir kata semoga skripsi ini dapat memberikan manfaat bagi pembaca umumnya dan penulis khususnya.

Yogyakarta, 10 Desember 2014

Ifan Candra Kusuma
10.11.4433

DAFTAR ISI

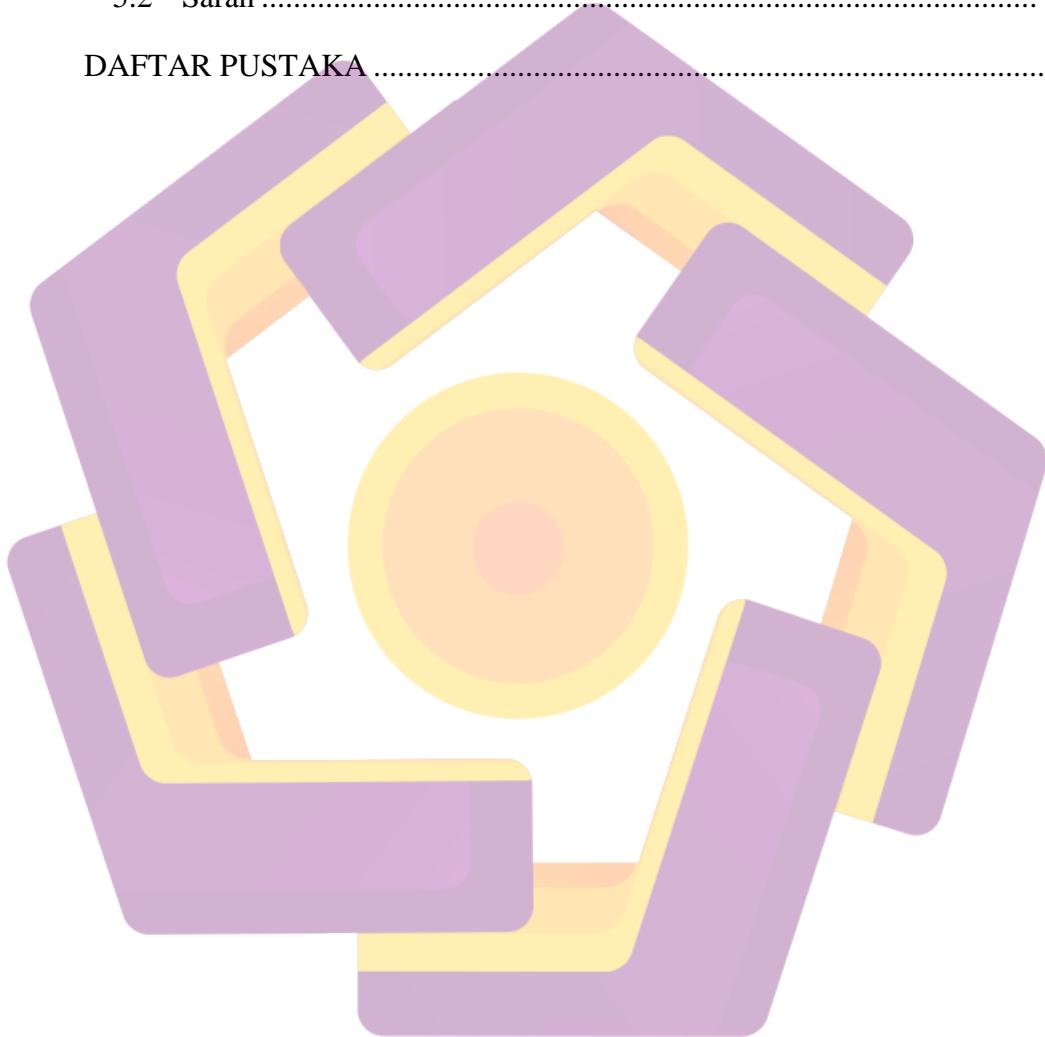
COVER	i
PERNYATAAN.....	iv
MOTTO	v
PERSEMBAHAN.....	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR	xiv
DAFTAR TABEL.....	xvi
INTISARI.....	xvii
ABSTRACT.....	xviii
BAB I.....	1
PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.5.1 Bagi penulis	4
2.5.1 Bagi masyarakat	4
1.6 Metodologi penelitian	5
1.7 Sistematika Penulisan	6
BAB II.....	8
LANDASAN TEORI.....	8

2.1	Tinjauan Pustaka.....	8
2.2	Pengertian Sistem	9
2.2.1	Karakteristik Sistem	9
2.3	Analisis Sistem	12
2.3.1	Keahlian Analisis	12
2.3.2	Keahlian teknis	13
2.3.3	Keahlian manajerial.....	13
2.3.4	Interpersonal skills	14
2.4	Tahap Analisis	15
2.5	Keamanan Jaringan.....	17
2.5.1	OSI.....	18
2.5.1.1	7 Layer model OSI.....	18
2.5.2	Prinsip keamanan jaringan	25
2.5.3	Alasan Keamanan Jaringan	26
2.6	Wi-Fi.....	27
2.7	Ruang Lingkup	28
2.8	Keamanan Wireless	29
2.8.1	Klasifikasi serangan	31
2.8.2	Service Set ID (SSID)	31
2.8.3	WEP.....	32
2.8.4	WPA	33
2.8.5	TKIP	34
2.8.6	WPA2	35
2.9	Acess Point	35
2.9.1	Inkripsi.....	36

2.9.2	DHCP	36
2.9.3	TCP/IP	37
2.9.4	Subnet Mask	39
2.9.5	NAT dan SPI	40
2.9.5.1	NAT.....	40
2.9.5.2	SPI.....	44
2.10	Kelemahan Jaringan Wireless.....	44
2.10.1	Kelemahan <i>Wireless</i> pada Lapisan Fisik	45
2.10.2	Kelemahan pada Lapisan MAC (Data Layer)	47
2.10.3	Contoh Serangan.....	47
2.10.4	Peranti Analisis dan Hacking Wireless.....	50
BAB III	54
METODOLOGI PENELITIAN	54
3.1	Metode Pengumpulan Data.....	54
3.2	Objek Penelitian.....	55
3.3	Analisis Masalah.....	56
3.3.1	Analisis Kondisi Lingkungan	56
3.3.1.1	Analisis Kondisi Lingkungan Fisik.....	56
3.3.1.2	Analisis Kondisi Lingkungan Non Fisik.....	57
3.3.2	Analisis Kelemahan Sistem.....	58
3.4	Solusi Terhadap Masalah.....	59
3.5	Analisis kebutuhan.....	59
3.5.1	Analisis Kebutuhan Perangkat Keras	59
3.5.2	Analisis Kebutuhan Perangkat lunak.....	63
3.5.3	Analisis Kebutuhan Sumber Daya Manusia (SDM)	63

3.6 Analisis Kelayakan	64
3.6.1 Kelayakan Hukum.....	64
3.6.2 Kelayakan Teknologi	64
3.6.2.1 Simulasi Serangan.....	64
3.6.2.2 Hasil yang diharapkan metode Sniffing.....	66
BAB IV	67
IMPLEMENTASI DAN PEMBAHASAN.....	67
4.1 Implementasi dan Pembahasan Evaluasi Lapangan	67
4.1.1 Tampilan Hasil Evaluasi	67
4.1.1.1 Plasa Telkom Ngawi	67
4.1.1.2 UPT alun-alun Ngawi.....	71
4.1.2 Analisis Perbandingan.....	74
4.1.2.1 Signal Strength.....	76
4.1.2.2 Interferensi Co-Channel.....	76
4.1.2.3 Overlapping.....	77
4.2 Hasil Analisis.....	78
4.2.1 Plasa Telkom Ngawi	78
4.2.2 UPT Alun-Alun Ngawi.....	80
4.3 Kuesioner.....	82
4.3.1 Karakteristik Responden	83
4.4 Pengujian Simulasi	92
4.4.1 Pengujian Sniffing.....	92
4.4.1.1 User Penyerang	92
4.4.1.2 User korban	93
4.5 Hasil Simulasi.....	95

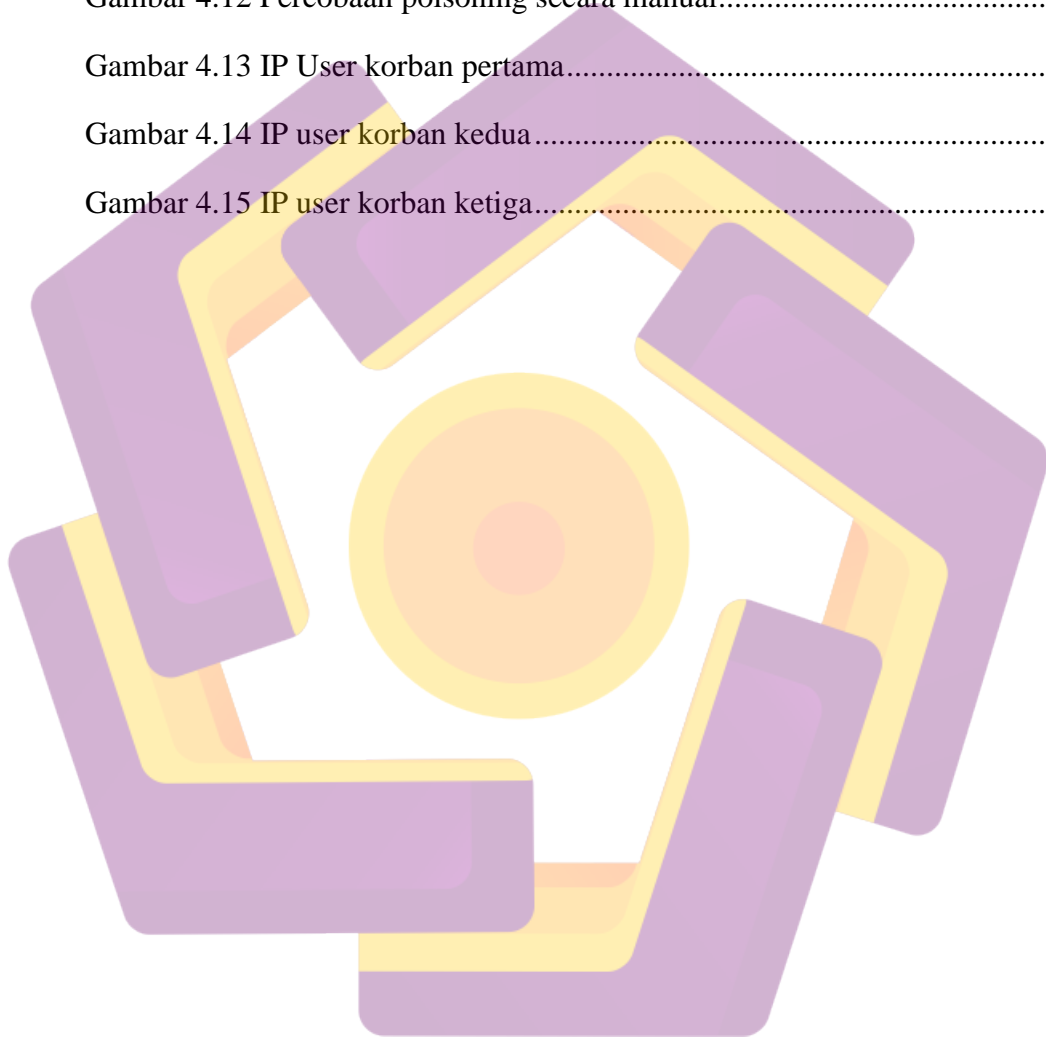
4.6 Laporan	96
BAB V.....	100
PENUTUP.....	100
5.1 Kesimpulan	100
5.2 Saran	100
DAFTAR PUSTAKA	102



DAFTAR GAMBAR

Gambar 2.1 Model OSI.....	19
Gambar 2.2 Spesifikasi Wi-fi.....	28
Gambar 2.3 Korelasi Antara TCP IP dan model OSI.....	39
Gambar 2.4 Static NAT.....	41
Gambar 2.5 Dynamic NAT.....	43
Gambar 2.6 Masquerading NAT.....	44
Gambar 2.7 Session Hijacking.....	48
Gambar 2.8 Man in the middle attack.....	49
Gambar 2.9 Replay Attack.....	50
Gambar 2.10 Aplikasi Ekahau HeatMapper.....	51
Gambar 2.11 Aplikasi <i>inSSIDer</i>	52
Gambar 2.12 Aplikasi Cain & Abel.....	53
Gambar 3.1 Denah Bangunan dan Halaman.....	56
Gambar 3.2 Denah Bangunan dan Halaman UPT.....	57
Gambar 3.3 Metode Sniffing.....	65
Gambar 4.1 Letak Pengambilan RSSI di Plasa Telkom Ngawi.....	68
Gambar 4.2 Coverage Visualitazion Plasa Telkom Ngawi.....	70
Gambar 4.3 Letak Pengambilan RSSI di UPT Ngawi.....	71
Gambar 4.4 Coverage Visualitazion UPT Ngawi.....	73
Gambar 4.5 UPT Ngawi.....	75
Gambar 4.6 Plasa Telkom Ngawi.....	75
Gambar 4.7 Diagram Signal Strength.....	76

Gambar 4.8 Presentase Diagram Interferensi Co-Channel	77
Gambar 4.9 Overlapping.....	78
Gambar 4.10 Pemindahan Posisi AP di UPT Ngawi.....	81
Gambar 4.11 konfigurasi interface penyerang.....	92
Gambar 4.12 Percobaan poisoning secara manual.....	93
Gambar 4.13 IP User korban pertama.....	94
Gambar 4.14 IP user korban kedua.....	94
Gambar 4.15 IP user korban ketiga.....	95



DAFTAR TABEL

Tabel 2.1 Segmen jaringan.....	40
Tabel 2.2 IP address private	41
Tabel 3.1 Analisis Kondisi Lingkungan Non Fisik.....	58
Tabel 3.2 Spesifikasi Wireless Router TD-W8961ND.....	60
Tabel 3.3 Spesifikasi Access Point Cisco Aironet 1552S/3500 series	61
Tabel 3.4 Spesifikasi Personal Computer (PC) / Notebook 1.....	62
Tabel 3.5 Spesifikasi Personal Computer (PC) / Notebook 2.....	62
Tabel 4.1 Pengukuran Plasa Telkom Ngawi.....	68
Tabel 4.2 Pengukuran UPT Ngawi	72
Tabel 4.3 Kuesioner	82
Tabel 4.4 Usia Responden	83
Tabel 4.5 Jenis Kelamin.....	84
Tabel 4.6 Latar Belakang Pekerjaan	84
Tabel 4.7 Penggunaan Dalam 1 Minggu.....	85
Tabel 4.8 Lama Waktu Penggunaan	86
Tabel 4.9 Waktu Penggunaan	87
Tabel 4.10 Biaya Pengeluaran Bulanan	87
Tabel 4.11 Alamat Yang Paling Sering Dikunjungi.	88
Tabel 4.12 Alasan Memilih wifi.id	89
Tabel 4.13 Kepuasan Pelanggan	90
Tabel 4.14 Jenis Paket.....	91
Tabel 4.15 Laporan	96

INTISARI

Masalah terbesar bagi infrastruktur nirkabel terutama yang membuka akses untuk umum seperti hotspot adalah, sistem koneksi dan autentikasi bagi pengguna. Dimana autentikasi dibutuhkan bagi pengguna nirkabel agar mereka dapat terhubung dengan jaringan nirkabel secara legal. Autentikasi juga dibutuhkan agar pengguna dapat memanfaatkan semua fasilitas yang telah disediakan oleh penyedia jaringan nirkabel.

Permasalahan yang biasa timbul dalam menangani jaringan nirkabel yaitu lemahnya sistem autentifikasi pada jaringan nirkabel yang tidak menggunakan metode enkripsi, berkembangnya penyerangan menggunakan MAC Address spoofing, keterbatasan MAC Address filtering pada perangkat Access Point, dan pendataan pengguna jaringan nirkabel yang tidak terpusat.

Untuk mengatasinya, penulis melakukan pengaturan terhadap fasilitas jaringan nirkabel agar dapat terbentuk sebuah jaringan nirkabel yang aman dengan melakukan analisa untuk autentifikasi dan otorisasi hak akses. Serta penerapan beberapa aplikasi pada jaringan nirkabel untuk lebih meningkatkan keamanan dan kenyamanan saat pengguna melakukan koneksi dan autentikasi terhadap penggunaan jaringan nirkabel. Diharapkan bermanfaat untuk mengendalikan dan mengontrol penggunaan jaringan nirkabel.

Kata kunci: nirkabel, jaringan, keamanan



ABSTRACT

The problem for the wireless infrastructure, especially the open access to public hotspots is, connection and authentication system for users. Where authentication is required for wireless users so they can connect to wireless networks legally. Authentication is also needed so that users can take advantage of all the facilities provided by the wireless network provider.

Problems that arise in dealing with wireless networks are weak authentication systems on wireless networks that do not use encryption methods, the development of assault using a MAC address spoofing, MAC Address filtering limitations on the Access Point device, and data wireless network users are not centralized.

To overcome this, the authors make arrangements for wireless networking facilities in order to form a secure wireless network analysis server for authorization authentication and access rights. And implementation of several applications on the wireless network to further increase the safety and convenience when users connect and authenticate to the use of wireless networks.

Keywords: wireless, network, security

