

ANALISA KEAMANAN JARINGAN WIRELESS LOCAL AREA NETWORK DENGAN ACCESS POINT TP-LINK WA500G



SKRIPSI

Disusun sebagai salah satu syarat menyelesaikan Jenjang Strata I
pada Program Studi Teknik Informatika Fakultas Komunikasi dan Informatika
Universitas Muhammadiyah Surakarta

Oleh:

Agung Nugroho

NIM : L200080023

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS MUHAMMADIYAH SURAKARTA**

2012

HALAMAN PERSETUJUAN

Skripsi dengan judul

**ANALISA KEAMANAN JARINGAN WIRELESS LOCAL AREA NETWORK
DENGAN ACCESS POINT TP-LINK WA500G**


ini telah diperiksa, disetujui dan disahkan pada :

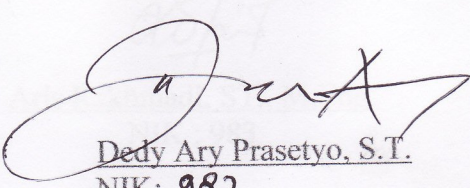
Hari :

Tanggal :

Pembimbing I

Pembimbing II


Fajar Suryawan, S.T., M.Eng.Sc.Ph.D.
NIK:924


Dedy Ary Prasetyo, S.T.
NIK: 982

HALAMAN PENGESAHAN

ANALISA KEAMANAN JARINGAN WIRELESS LOCAL AREA NETWORK DENGAN ACCESS POINT TP-LINK WA500G

dipersiapkan dan disusun oleh

Agung Nugroho

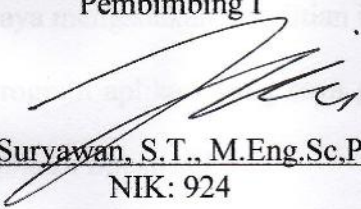
NIM : L200080023

telah dipertahankan di depan Dewan Penguji

pada tanggal 13 Juli 2012.....

Susunan Dewan Penguji

Pembimbing I



Fajar Suryawan, S.T., M.Eng.Sc.Ph.D.

NIK: 924

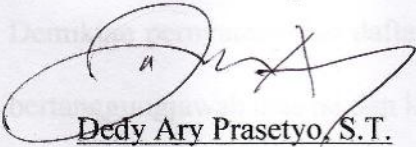
Anggota Dewan Penguji Lain



Jan Wantoro, S.T.

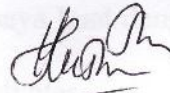
NIK: 200.1304

Pembimbing II



Dedy Ary Prasetyo, S.T.

NIK:



Husni Thamrin, S.T, MT., Ph.D.

NIK : 706

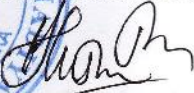
Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar sarjana

Tanggal 13 Juli 2012.....

Dekan

Fakultas Komunikasi dan Informatika

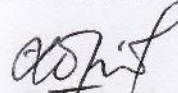


Husni Thamrin, S.T, MT., Ph.D.

NIK : 706

Ketua Program Studi

Teknik Informatika



Aris Rakhmadi, ST., M.Eng.

NIK : 983



DAFTAR KONTRIBUSI

MOTTO :

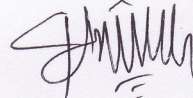
Dengan ini saya menyatakan bahwa skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Berikut saya sampaikan daftar kontribusi dalam penyusunan skripsi:

1. Saya mengadakan penelitian ini berdasarkan informasi dari buku.
2. Program aplikasi yang saya gunakan semua terdapat dalam *Operating System Ubuntu Backtrack 4.2*.
3. *Access point* yang digunakan adalah TP-LINK WA500G.

Demikian pernyataan dan daftar kontribusi ini saya buat dengan sejujurnya. Saya bertanggungjawab atas isi dan kebenaran daftar di atas.

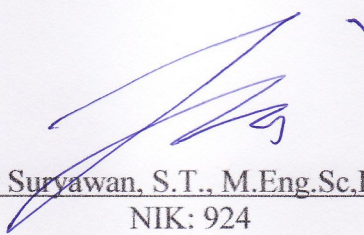
Surakarta, Mei 2012



Agung Nugroho

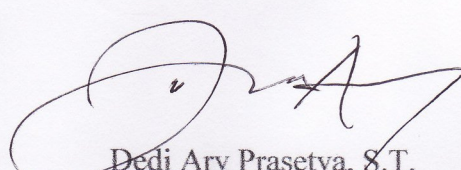
Mengetahui:

Pembimbing I



Fajar Suryawan, S.T., M.Eng.Sc,Ph.D
NIK: 924

Pembimbing II



Dedi Ary Prasetya, S.T.
NIK: 982

MOTTO DAN PERSEMBAHAN

MOTTO :

“Muliakanlah ke dua Orang Tuamu, karena Merekalah jalan kesuksesanmu”.

“Do the best”.

”Apa yang kamu yakini, adalah apa yang kelak akan kamu dapatkan kelak”.

“ALLOH SWT selalu memberikan jalan terbaik untuk umat-NYA”

-Penulis

PERSEMBAHAN

1. Ibu, Bapak tercinta yang selalu mendukung, mendoakan, membiayai, dan memberikan semangat terus sampai saat ini sehingga aku bisa menyelesaikan skripsi ini.
Terimakasih
2. Buat kakak-kakak saya mbak Mamik dan mas Sugeng serta om Sabar yang selalu berbagi pengalaman hidup mereka.
3. Buat sahabat spesial saya dari semester pertama Ardi, Budi, Radix dan Fajar, terima kasih atas kebersamaannya selama ini.
4. Buat para wanita yang pernah hadir dalam hidup saya ^^.
5. Buat temen-temen kos Kevin, You Rock Guys.
6. Temen-temen Teknik Informatika khususnya angkatan 2008 yang tidak dapat disebutkan satu-persatu, terima kasih telah bersedia berbagi ilmu dan pengalamannya.
7. Semua pihak yang telah membantuku yang tidak dapat aku sebutkan satu-persatu.

KATA PENGANTAR

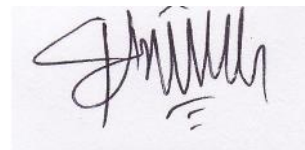
Puji syukur penulis panjatkan ke hadirat Allah SWT, yang telah melimpahkan taufik, hidayah dan rahmat-Nya sehingga skripsi dengan judul “Analisa Keamanan Jaringan Wireless Local Area Network Dengan Acces Point TP-LINK WA 500G” dapat diselesaikan dengan baik. Skripsi ini dapat terselesaikan berkat bantuan dari berbagai pihak, oleh karena itu pada kesempatan ini penulis menyampaikan terima kasih dan penghargaan kepada :

1. Bapak Husni Thamrin, S.T, MT., Ph.D. selaku Dekan Fakultas Komunikasi dan Informatika yang telah melayani dan memberikan fasilitas bagi kelancaran studi.
2. Bapak Aris Rakhmadi, ST., M.Eng. selaku ketua jurusan Teknik Informatika.
3. Bapak Fajar Suryawan, S.T., M.Eng.Sc,Ph.D selaku pembimbing I dan Bapak Dedy Ary Prasetyo, S.T. selaku pembimbing II yang penuh kesabaran di sela-sela kesibukannya selalu memberi petunjuk, bimbingan, saran-saran, serta dorongan bagi penyelesaian skripsi ini.
4. Segenap dosen penguji pada seminar proposal dan pra pendadaran yang telah memberikan saran dan masukan dalam penyusunan skripsi ini.
5. Bapak dan ibu dosen pengampu mata kuliah pada Program Studi Teknik Informatikan yang telah memberikan bekal ilmu yang sangat bermanfaat bagi penulis.
6. Segenap Staf / Karyawan pada Program Studi teknik Informatika yang telah melayani dan memberikan fasilitas bagi kelancaran studi.

7. Rekan-rekan Teknik Informatika khususnya angkatan 2008 yang tiada henti memberikan dorongan dan dukungan.

Semoga Allah SWT berkenan untuk memberikan balasan yang sesuai dengan budi baik yang telah mereka berikan. Penulis berharap semoga skripsi ini dapat bermanfaat bagi pengembangan pendidikan selanjutnya.

Surakarta, Mei 2012

A handwritten signature in black ink, appearing to be 'F. M. H.', written on a light-colored background.

Penulis

DAFTAR ISI

Halaman Judul	i
Halaman Persetujuan	ii
Halaman Pengesahan	iii
Daftar Kontribusi	iv
Motto dan Persembahan	v
Kata Pengantar	vii
Daftar Isi	ix
Daftar Tabel	xii
Daftar Gambar	xiii
Abstraksi	xv
BAB I PENDAHULUAN	1
1.1. Latar Belakang Masalah.....	1
1.2. Rumusan Masalah	2
1.3. Batasan Masalah	2
1.4. Tujuan Penelitian	3
1.5. Manfaat Penelitian	3
1.6. Sistematika Penulisan.....	3
BAB II TINJAUAN PUSTAKA	5
2.1. Telaah Penelitian	5
2.2. Landasan Teori	6
2.2.1. Internet	6
2.2.2. Wireless LAN	8

	2.2.3. TCP/IP	22
BAB III	METODE PENELITIAN	29
	1.1 Waktu dan Tempat Penelitian	29
	1.2 Alat dan Bahan	29
	3.2.1. Hardware (Perangkat Keras)	29
	2.2.1. Software (Perangkat Lunak)	29
	1.3 Alur Penelitian	30
	1.4 Analisis Skema Pengujian	32
	3.4.1 Skema Rancangan Pengujian Wireless	32
	3.4.2 Analisa Pengujian Keamanan	34
	A. Reveal SSID	36
	B. Mac Spoofing	41
	C. Cracking WEP	45
	D. Cracking WPA/WPA2 PSK	53
BAB IV	HASIL DAN PEMBAHASAN	59
	4.1. Hasil Penelitian	59
	4.2. Analisis Hasil Penelitian	59
	4.2.1. Reveal SSID	59
	4.2.2. Mac Spoofing	61
	4.2.3. Cracking WEP	62
	4.2.4. Cracking WPA/WPA2 PSK	64
	4.3 Peningkatan Keamanan	68
BAB V	PENUTUP	71
	A. Kesimpulan	71

B. Saran	72
DAFTAR PUSTAKA	73

DAFTAR TABEL

Tabel 2.1 Subnet Mask Default	26
Tabel 2.2 Subnet host efektif kelas C	26
Tabel 3.1 Parameter Pengujian	33
Tabel 3.2 Spesifikasi access point	33
Tabel 3.3 Spesifikasi client dan penyusup.....	33
Tabel 4.1 Hasil Pengujian Keamanan Access Point	67

DAFTAR GAMBAR

Gambar 3.1	Diagram alir percobaan	30
Gambar 3.2	Skema penyerangan.....	32
Gambar 3.3	Konfigurasi tanpa keamanan	34
Gambar 3.4	Diagram flowchart <i>reveal SSID</i>	36
Gambar 3.5	Non-aktif SSID <i>broadcast</i>	38
Gambar 3.6	Mengaktifkan <i>mode monitor</i>	38
Gambar 3.7	<i>Scanning wireless</i> dan <i>snifing</i>	39
Gambar 3.8	Serangan <i>deauthentication</i>	40
Gambar 3.9	Diagram flowchart MAC <i>spoofing</i>	41
Gambar 3.10	Mengaktifkan <i>Mac Filtering</i>	43
Gambar 3.11	Proses <i>Mac Spoofing</i>	44
Gambar 3.12	Diagram flowchart <i>Cracking WEP</i>	45
Gambar 3.13	Mengaktifkan keamanan WEP	47
Gambar 3.14	Merekam paket <i>handshake</i>	48
Gambar 3.15	Serangan <i>fake authentication</i>	49
Gambar 3.16	Hasil <i>fake authentication</i>	50
Gambar 3.17	<i>injeksi paket dengan aireplay-ng</i>	50
Gambar 3.18	<i>crack wep</i>	51
Gambar 3.19	Proses <i>crack WEP</i>	52
Gambar 3.20	Diagram flowchart <i>Cracking WPA/WPA2 PSK</i>	53
Gambar 3.21	Mengaktifkan WPA/WPA2 PSK	55
Gambar 3.22	Serangan <i>dictionary attack</i>	57
Gambar 3.23	Proses <i>crack WPA/WPA2 PSK</i>	58

Gambar 4.1	Mendapatkan <i>SSID</i>	51
Gambar 4.2	Hasil <i>Mac Spoofing</i>	39
Gambar 4.3	Hasil <i>crack</i> WEP	55
Gambar 4.4	Hasil <i>crack</i> WPA/WPA2 PSK.....	56
Gambar 4.5	Setting peningkatan Keamanan	56
Gambar 4.6	Hasil perbaikan keamanan.....	56

ABSTRAKSI

Perkembangan teknologi *wireless* sangat berkembang, selain memiliki keunggulan dalam hal *fleksibilitas*, *wireless* juga memiliki celah kelemahan. Maka diperlukan identifikasi kelemahan keamanan pada *wireless* untuk lebih baik kedepannya dalam meningkatkan keamanan *wireless*.

Pada pengujian ini akan dilakukan pengujian terhadap keamanan pada jaringan *wireless* dari sisi keamanan *access point*, dan *access point* yang digunakan adalah *TP-LINK WA500G*. Metode konsep yang digunakan adalah *wireless hacking*, pengujiannya diantaranya meliputi *reveal SSID (Service Set Identifier)*, *MAC address spoofing*, *crack WEP (Wired Equivalent Privacy)*, *crack WPA/WPA2 PSK (Wifi Protected Access Pre-Shared Key)*.

Dari hasil pengujian terhadap celah keamanan *access point TP-LINK WA500G* dapat memberikan pemahaman terhadap celah keamanannya dan cara untuk pencegahan *wireless hacking*.

Kata Kunci : wireless, SSID, WEP, Mac address, WPA/WPA2 PSK.