

**ANALISIS KEAMANAN JARINGAN (WIFI) TERHADAP SERANGAN
PACKET SNIFFING**

SKRIPSI



disusun oleh

Wardi Manik

14.11.8038

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019**

**ANALISIS KEAMANAN JARINGAN (WIFI) TERHADAP SERANGAN
PACKET SNIFFING**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Wardi Manik

14.11.8038

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2019

PERSETUJUAN

SKRIPSI

**ANALISIS KEAMANAN JARINGAN (WIFI) TERHADAP SERANGAN
PACKET SNIFFING**

yang dipersiapkan dan disusun oleh

Wardi Manik

14.11.8038

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 22 Februari 2017

Dosen Pembimbing,



Joko Dwi Santoso, M.Kom

NIK. 190302181

PENGESAHAN

SKRIPSI

**ANALISIS KEAMANAN JARINGAN (WIFI) TERHADAP SERANGAN
PACKET SNIFFING**

yang dipersiapkan dan disusun oleh

Wardi Manik

14.11.8038

telah dipertahankan didepan Dewan Penguji
pada tanggal 22 February 2019

Susunan Dewan Penguji

Nama Penguji

Bayu Setiaji, M.Kom
NIK. 190302216

Ike Verawanti, M.Kom
NIK. 190302237

Joko Dwi Santoso, M.Kom
NIK. 190302181

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Serjana Komputer
Tanggal 22 February 2019

DEKAN FAKULTAS ILMU KOMPUTER



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

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 tinggi manapun, 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.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 15 March 2019

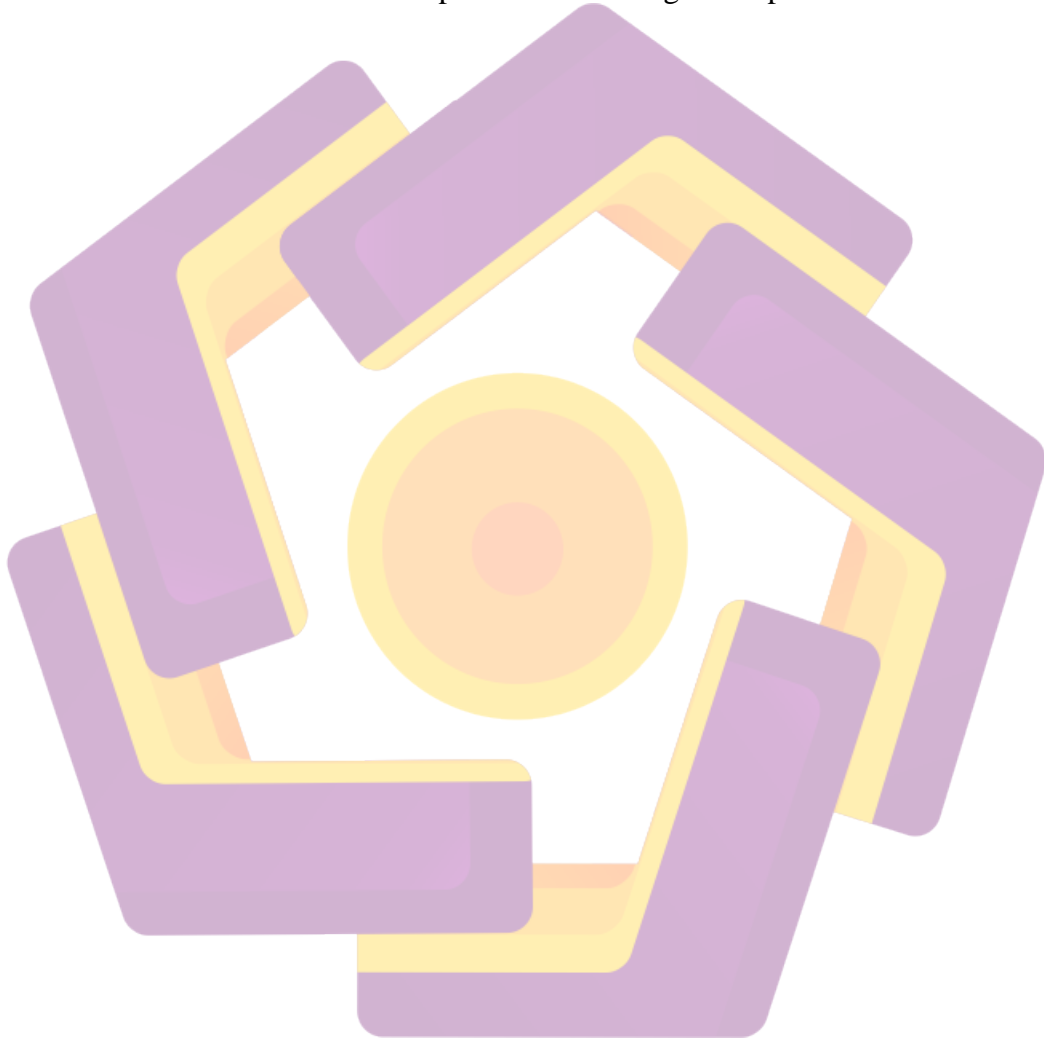


Wardi Manik
NIM. 14.11.8038

MOTTO

Yakin adalah kunci dari semua segala untuk menuju kesuksesan.

Dengan bermodal yakin semua halangan yang menghalang akan kita lewati
dan penumbuh semangat hidup.



PERSEMBAHAN

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa yang selalu menyertai sepanjang hidupku.

Ucapan terima kasih penulis sampaikan kepada Bapak Joko Dwi Santoso, M.Kom selaku dosen pembimbing yang telah memberikan panduan serta arahan dengan penuh kepercayaan kepada penulis untuk menyempurnakan skripsi ini. Ucapan terimakasih juga ditunjukkan kepada Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta, Ibu Krisnawarti, S.SI., M.T. dan Prof. Dr. M. Suyanto, M.M. selaku ketua Universitas Amikom Yogyakarta.

Tidak terlupakan keluarga, Bapak, Mamak, Kakak, Adik, Pacar yang selalu memberikan doa dan support. Dan semua teman-teman yang tidak bisa saya sebutkan satu persatu yang telah membantu untuk kelancaran dalam pembuatan skripsi ini. Semoga Tuhan membalasnya untuk semua.

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa yang telah memberikan nikmat, rahmat, serta karunia nya sehingga penulis berkesempatan untuk menulis skripsi dengan judul “ **ANALISIS KEAMANAN JARINGAN (WIFI) TERHADAP SERANGAN PACKET SNIFFING** ” dengan baik. Penulis ini diajukan untuk memenuhi salah satu syarat kelulusan dalam jenjang perkuliahan Strata 1 Universitas Amikom Yogyakarta.

Dalam penyusunannya, penulis memperoleh banyak bantuan dari berbagai pihak, oleh karena itu penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. M. Suyanto,MM selaku rektor Universitas Amikom Yogyakarta.
2. Ibu Krisnawati, S.Si, MT selaku Ketua Jurusan S1-Sistem Informasi Universitas Amikom Yogyakarta.
3. Bapak Joko Dwi Santoso, M.Kom selaku dosen pembimbing yang telah memberikan saran, arahan, bimbingan, motivasi dan waktu yang sangat membantu dalam pembuatan skripsi ini.
4. Bapak/Ibu dosen, staff dan karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu dan bantuan yang bermanfaat.
5. Echi Simangunsong telah memberi semangat dan yang telah memberi waktunya untuk membantu penulis.

6. Doa semua orang baik yang telah disebutkan maupun yang tidak disebutkan.

Tidak ada kata yang sempurna dalam hal apapun. Begitupun dengan laporan Skripsi ini yang masih jauh dari kata sempurna. Semoga kritik dan saran yang diberikan dapat membangun untuk lebih baik lagi. Semoga laporan ini bermanfaat bagi pembaca pada umumnya dan penulis pada khususnya. Amin

Yogyakarta, 14 Maret 2019



Penulis

DAFTAR ISI

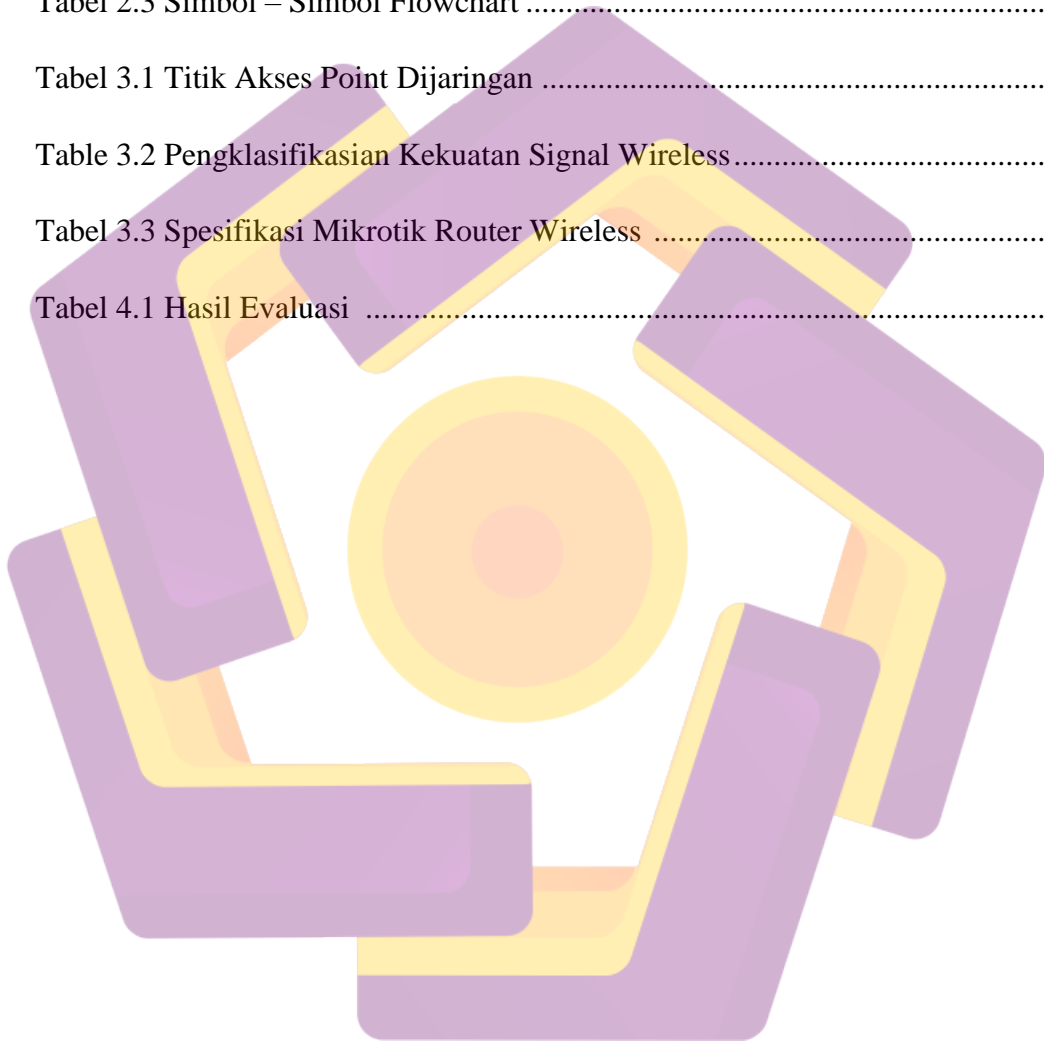
JUDUL.....	i
PERSETUJUAN.....	iii
PENGESAHAN.....	iv
MOTTO.....	vi
PERSEMBAHAN.....	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR.....	xiv
INTISARI.....	xvi
ABSTRACT.....	xvii
BAB I. Pendahuluan.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Metode Penelitian.....	3
1.6.1 Metode SDLC.....	3
1.7 Sistematika Penulisan.....	4
BAB II. Landasan Teori.....	5
2.1 Tinjauan Pustaka.....	5
2.2 Jaringan Komputer.....	8
2.3 Jaringan Wireless.....	8

2.4	Kemanan Jaringan <i>Wireless</i>	10
2.4.1	Ancaman	10
2.4.2	Kelemahan.....	12
2.5	Jenis – jenis Ancaman Keamanan Jaringan	12
2.5.1	Packet Sniffer	12
2.5.2	ARP spoofing / ARP poisoning	13
2.5.3	Probe	14
2.5.4	Scan.....	14
2.5.5	Account Compromise	14
2.5.6	Root Compromise	15
2.5.7	Denial Of Service (Dos).....	15
2.6	Keamanan Data.....	16
2.7	Radius.....	17
2.8	InSSIDer.....	18
2.9	Wireshark.....	18
2.10	Metode SPDLC	19
2.11	Flowchart Analisis.....	20
BAB III. ANALISIS DAN PERANCANGAN SISTEM		21
3.1	Tinjauan Umum Objek Penelitian.....	23
3.1.1	Gambaran Umum.....	23
3.2	Identifikasi Masalah.....	24
3.2.1	Memonitor Lalu Lintas Jaringan.....	24
3.3	Analisa Keamanan Wireless	27
3.3.1	Proses Sebelum Analisa Keamanan	27
3.3.2	Proses Analisa	28

3.3.3	Penanganan Masalah.....	32
3.3.4	Design <i>Wireless</i>	33
BAB IV IMPLEMENTASI DAN PEMBAHASA		39
4.1	Implementasi.....	39
4.1.1	Konfigurasi Awal Router.....	39
4.2	Konfiurasi Hotspot dan Radius Mikrotik.....	51
4.2.1	Inatallsi Package Unsermanager.....	51
4.2.2	Konfigurasi Server Radius.....	51
4.2.3	Konfigurasi Hotspot Mikrotik.....	52
4.2.4	Konfigurasi Hotspot Server.....	53
4.3	Konfigurasi Mikrotik Unsermanager.....	54
4.3.1	Menganti Password Unsermanager.....	54
4.3.2	Menghubungkan Konfigurasi Router Pada User manager.....55ss	55
4.3.3	Profile Tamu dan Limitasi.....	56
4.4	Audit Sistem Baru.....	58
4.4.1	Audit Sistem User Baru.....	58
4.5	Evaluasi Sistem Baru.....	60
BAB V PENUTUP.....		63
5.1	Kesimpulan.....	63
5.2	Saran	63
DAFTAR PUSTAKA.....		64
LAMPIRAN.....		

DAFTAR TABEL

Tabel 2.1 Tinjau Pustaka.....	6
Tabel 2.2 Daftar Keluarga 802.11.....	9
Tabel 2.3 Simbol – Simbol Flowchart.....	20
Tabel 3.1 Titik Akses Point Dijaringan.....	25
Table 3.2 Pengklasifikasian Kekuatan Signal Wireless.....	25
Tabel 3.3 Spesifikasi Mikrotik Router Wireless.....	37
Tabel 4.1 Hasil Evaluasi.....	63



DAFTAR GAMBAR

Gambar 3.1 Hasil Capture Insider Pada Jaringan Wifi	25
Gambar 3.3 Laptop Asus A456u.....	27
Gambar 3.4 Capture Aplikasi Wireshark	28
Gambar 3.5 Capture Percobaan.....	29
Gambar 3.6 Pencarian IP Target dengan CMD	29
Gambar 3.7 Capture Monitoring Jaringan	30
Gambar 3.8 Capture Lalu Lintas Ip Target	31
Gambar 3.9 Hasil Monitoring Target.....	32
Gambar 3.10 Topologi Jaringan Lama.....	33
Gambar 3.11 Topologi Jaringan Baru	34
Gambar 3.12 Mikrotik Router Wireless	35
Gambar 3.13 Modem Huawei GPON HG8245H	37
Gambar 3.14 Kabel UTP.....	38
Gambar 4.1 Login Router Mikrotik via Winbox	40
Gambar 4.2 Proses Remote Pada Mikrotik Berhasil.....	41
Gambar 4.3 Konfigurasi Hak Akses User.....	42
Gambar 4.4 Pengganti Nama Interface	43
Gambar 4.5 Pengganti Nama Interface Berhasil.....	43
Gambar 4.6 Pengganti Nama SSID.....	44
Gambar 4.7 Konfigurasi DHCP Client	44
Gambar 4.8 Konfigurasi DHCP Client Berhasil	45
Gambar 4.9 Konfigurasi IP Address Berhasil.....	45
Gambar 4.10 Konfigurasi NAT.....	46
Gambar 4.11 Konfigurasi ICMP	47
Gambar 4.12 Konfigurasi IP Pool.....	48
Gambar 4.13 Konfigurasi IP Pool Berhasil.....	48
Gambar 4.14 Konfigurasi Netork DHCP Server.....	49

Gambar 4.15 Konfigurasi DHCP Server.....	50
Gambar 4.16 Konfigurasi DHCP Server Berhasil	50
Gamabr 4.17 Input Unsermanager ke Router	51
Gambar 4.18 Konfigurasi Radius.....	52
Gambar 4.19 Konfigurasi Radius Server	52
Gambar 4.20 Konfigurasi Server Profile	53
Gambar 4.21 Konfigurasi Hotspot Server.....	54
Gambar 4.22 Halaman Login Unsermanager.....	55
Gambar 4.23 Login Unsermanager Berhasil.....	55
Gambar 4.24 Konfigurasi User Login dan Password Username	56
Gambar 4.25 Konfigurasi User Login dan Password Berhasil	56
Gambar 4.26 Pengisian IP dan Share Secret Unsermanager	57
Gambar 4.27 Membuat Profile Tamu	58
Gambar 4.28 Membuat Limitasi Pada Profile Tamu	58
Gambar 4.29 Input Data Username.....	59
Gambar 4.30 Proses Unser Login Hotspot Mikrotik	60
Gambar 4.31 Login Hotspot Mikrotik Berhasil	60
Gambar 4.32 Pencarian IP Target	61
Gambar 4.33 Username dan Password Target	62
Gambar 4.34 Memonitoring Jaringan	62
Gambar 4.35 Proses pencarian	63

INTISARI

Salah satu perkembangan dibidang telekomunikasi adalah penggunaan teknologi Nirkabel (wireless). Masalah yang dihadapi apabila menerapkan jaringan Wireless adalah isu tentang keamanannya. Banyak pihak yang masih mempertanyakan tentang keamanannya sehingga apabila ingin menerapkan jaringan wireless . maka harus mempertimbangkan sistem keamanan apa yang akan kita terapkan. Solusinya yang dilakukan adalah menerapkan *RADIUS(Remote Authentication Dial-in User Service) server*.

Radius merupakan protokol jaringan yang menjalankan service management Authentication, Authorization, dan Accounting (AAA) secara terpusat untuk user yang terkoneksi dan hendak menggunakan resource dalam jaringan.

MikroTik memiliki fitur radius server yang disebut *UserManager*. *UserManager* akan memudahkan ketika kita yang ingin membuat layanan jaringan yang didistribusikan secara luas, misal hotspot di cafe, mall, hotel dan sebagainya. Dengan menggunakan *UserManager* ini kita cukup membuat satu account user di router utama, dan account user tersebut bisa digunakan atau diakses dari router *DHCP/Wireless*.

Kata Kunci : *Radius, Mikrotik, AAA, UserManager, Management bandwidth,*

ABSTRACT

Wireless network is a local network without cables that is used to give a network connection for all users around the area by radio waves and microwave. Wireless network that are usually found are one of the service product such as communication service packet and data like a telephone (voice), internet (internet on fiber or high speed internet), and television service. Packet sniffing is a data theft technique that is done by monitoring and analyzing among the packet data which is transmitted from client computer into web server. By doing this method, the best solution against the problem can be expected. Based on the explanation above the problem formulation that occur is: How improve the safety of wireless network.

In this research, the researcher tried to analyze the main problem that occurs and tried to give knowledge and information to the users of wireless network in general about the risks of network without any security, and also gave the solution to improve the wireless network security. The research used SPDLC (Security Policy Development Life Cycle). There are some steps that are used such as the step of identification of problem, analysis, design, implementation, audit, and evaluation.

The result of the research is about the way that support the enhancement of the security of wireless network by using micro tic. By the use of microtic, the right of accessing for the users will be limited, build a new topology with a higher level of security, and also cover the space that is possible for the possible attack against the network. By dong the steps, the security of wireless network in boarding house area can be improved.

Keywords: Wireless, SPDLC, Mikrotik, Radius