

**ANALISA KEAMANAN JARINGAN DENGAN MENGGUNAKAN
REMOTE AUTENTIFIKASI DIAL IN USER SERVICE
(RADIUS) SERVER DI PT. ASABA**

SKRIPSI

Program Studi TEKNIK INFORMATIKA



OLEH:

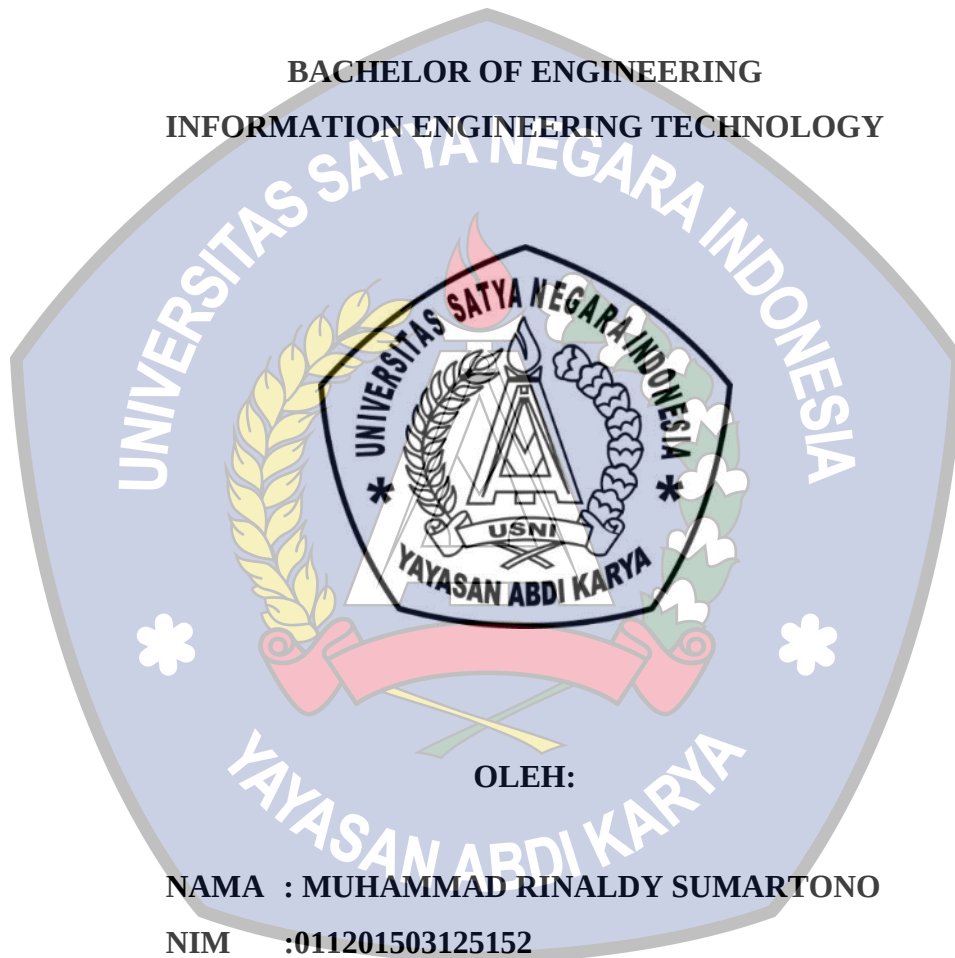
NAMA : MUHAMMAD RINALDY SUMARTONO
NIM : 011201503125152

FAKULTAS TEKNIK
UNIVERSITAS SATYA NEGARA INDONESIA
JAKARTA
2017

**ANALYSIS OF NETWORK SECURITY BY USING REMOTE
AUTHENTICATION DIAL IN USER SERVICE (RADIUS)
SERVER IN PT. ASABA**

**UNDERGRADUATE THESIS
Proposed As One Of Terms To Obtain Degree**

**BACHELOR OF ENGINEERING
INFORMATION ENGINEERING TECHNOLOGY**



OLEH:

NAMA : MUHAMMAD RINALDY SUMARTONO

NIM :011201503125152

**FAKULTAS TEKNIK
UNIVERSITAS SATYA NEGARA INDONESIA
JAKARTA**

2017

**ANALISA KEAMANAN JARINGAN DENGAN MENGGUNAKAN
REMOTE AUTENTIFIKASI DIAL IN USER SERVICE
(RADIUS) SERVER DI PT. ASABA**

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar
SARJANA TEKNIK
PROGRAM STUDI TEKNIK INFORMATIKA**



BY:

NAME : MUHAMMAD RINALDY SUMARTONO

ID : 011201503125152

FACULTY OF ENGINEERING

UNIVERSITY OF SATYA NEGARA INDONESIA

JAKARTA

2017

KATA PENGANTAR

Dengan mengucapkan puji dan syukur kehadiran Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan penyusunan skripsi yang berjudul **“ANALISA KEAMANAN JARINGAN DENGAN MENGGUNAKAN *REMOTE AUTENTIFIKASI DIAL IN USER SERVICE (RADIUS) SERVER* DI PT. ASABA”**

Adapun maksud penyusunan skripsi ini adalah untuk memenuhi syarat dalam memperoleh gelar sarjana jenjang Strata 1 (Satu) program studi Teknik Informatika Fakultas Teknik Universitas Satya Negara Indonesia.

Dalam penulisan skripsi ini penulis banyak mendapatkan dukungan dan bantuan dari berbagai pihak yang sangat besar artinya bagi penulis. Oleh karena itu penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada :

1. Ibu Dr. Yusriani Sapta Dewi, M.Si. selaku Rektor Universitas Satya Negara Indonesia.
2. Ibu Ir. Nurhayati, M.Si. selaku Dekan Fakultas Teknik Universitas Satya Negara Indonesia.
3. Bapak Zulkifli, S.Kom., M.Kom. selaku Ketua Jurusan Teknik Informatika. Bapak Faizal Zuli, S.Kom., M.Kom. selaku pembimbing I yang telah meluangkan waktu dan pikiran untuk memberikan arahan yang terbaik sehingga skripsi ini selesai.

4. Bapak Safrizal, ST., MM., M.Kom. selaku pembimbing II yang telah meluangkan waktu dan pikiran untuk memberikan bimbingan dan arahnya yang terbaik sehingga skripsi ini dapat selesai.
5. Seluruh Dosen Universitas Satya Negara Indonesia beserta para stafnya, yang telah memberikan ilmu dan membantu selama masa pendidikan.
6. Kedua Orang tua dan Keluarga yang telah memberikan doa serta dukungan baik moril maupun materil.
7. Semua sahabat seperjuangan mahasiswa Teknik Informatika dan seluruh teman-teman Fakultas Teknik.
8. Para alumni Universitas Satya Negara Indonesia Fakultas Teknik Informatika.
9. Penulis menyadari sepenuhnya dan mengharapkan saran dan masukan yang bersifat membangun demi bertambah baiknya tulisan ini dimasa yang akan datang, dengan tujuan dapat bermanfaat bagi pihak – pihak yang terkait dengan penulisan ini dan bagi kita semua.

Jakarta, 28 Juli 2017

Muhammad Rinaldy Sumartono

ABSTRAK

Komunikasi tanpa kabel atau nirkabel telah menjadi kebutuhan dasar gaya hidup baru masyarakat informasi. LAN nirkabel yang lebih dikenal dengan jaringan Wi-Fi menjadi teknologi alternatif dan relatif lebih mudah diimplementasikan di lingkungan kerja, seperti di perkantoran, laboratorium komputer, dan sebagainya. Masalah yang dihadapi di PT. ASABA adalah isu tentang keamanannya. Apabila mengimplementasikan wireless LAN, maka harus mengimplementasikan pengguna yang tidak menerapkan sistem keamanan yang memadai, sehingga memungkinkan pengguna yang tidak berhak atau ilegal dapat masuk ke Jaringan *hotspot*. Sistem keamanan *wireless* yang memberikan keamanan yang lebih *secure* adalah dengan menggunakan sistem keamanan *Remote Autentifikasi Dial in User Service* (RADIUS) server. Tujuan dari penelitian ini adalah merancang dan membangun serta menganalisa sistem keamanan dengan menggunakan Radius Server karena sesuai dengan pokok bahasan yaitu Analisis, Implementasi, dan Monitoring.

Kata kunci : *Remote Autentifikasi Dial in User Service* (RADIUS), *Security Policy Development Life Cycle* (SPDLC).

ABSTRACT

Wireless or wireless communication has become a basic need of a new lifestyle of information society. Wireless LAN is better known as Wi-Fi network into alternative technology and relatively easier to implement in the work environment, such as in offices, computer labs, and so forth. The problem faced in PT. ASABA is the issue of security. When implementing a wireless LAN, it must implement a user who does not implement an adequate security system, allowing unauthorized or illegal users to enter the Hotspot network. A wireless security system that provides more secure security is by using the Remote Authentication Security System Dial in User Service (RADIUS) server. The purpose of this research is to design and build and analyze security system by using Radius Server as according to subject matter that is Analyze, Implementation, and Monitoring.

Key word : Remote Authentication Dial in User Service (RADIUS), Security Policy Development Life Cycle (SPDLC).

DAFTAR ISI

SURAT PERNYATAAN KARYA SENDIRI	i
LEMBAR PENGESAHAN SKRIPSI	ii
LEMBAR PENGESAHAN PENGUJI	iii
KATA PENGANTAR	Error! Bookmark not defined.
ABSTRAK	vi
DAFTAR ISI	vii
DAFTAR TABEL	x
DAFTAR GAMBAR	xi
BAB I	Error! Bookmark not defined.
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan dan Manfaat	3
1.4.1 Tujuan Penelitian	3
1.4.2 Manfaat	3
1.5 Sistematika Penulisan	3
BAB II	5
LANDASAN TEORI	5
2.1 Tinjauan Pusaka	5
2.2 Remote Authentication Dial In User Service (RADIUS)	6

2.3	Freeradius	9
2.4	Otentifikasi Dan Otorisasi Akses Jaringan.....	10
2.5	MAC Address.....	11
2.6	Eaves Dropping	11
2.7	IP Spoofing.....	12
2.8	Denial of Service	13
2.9	Distributed Denial of Service.....	15
2.10	Cara Kerja DDoS Attack	16
2.11	Metode Analisis SPDLC.....	17
BAB III		20
METODE PENELITIAN		20
3.1	Gambaran Umum Perusahaan	20
3.2	Analisa Sistem Berjalan	21
3.3	Usulan Pemecahan Masalah.....	21
3.4	Kerangka Berfikir.....	23
BAB IV		25
HASIL DAN PEMBAHASAN		25
4.1	Hasil.....	25
4.1.1	Identifikasi Masalah Wireless LAN.....	25
4.1.2	Pemantauan Lalu Lintas Jaringan	26
4.1.3	Membangun RADIUS Server	28

4.2	Pembahasan	62
4.2.1	Serangan sebelum instalasi radius.....	62
4.2.2	Serangan sesudah instalasi radius	70
4.2.3	Hasil Pengujian	78
4.3	Kesimpulan.....	81
4.4	Saran	81



DAFTAR TABEL

Tabel 4.1 Perangkat Keras	26
Tabel 4.2 Perangkat Lunak	27
Tabel 4.3 Sebelum Serangan.....	71
Tabel 4.4 Setelah Serangan.....	72



DAFTAR GAMBAR

Gambar 2.1 Konsep Distributed Denial of Service.....	13
Gambar 2.2 The Security Development Life Cycle.....	16
Gambar 3.1 Kerangka Berfikir.....	20
Gambar 4.1 Scan NetSurveyor.....	23
Gambar 4.2 Scan inSSIDer.....	24
Gambar 4.3 Alur Kerja Radius Server.....	25
Gambar 4.4 Setting LAN.....	28
Gambar 4.5 Tampilan Router TP-LINK 3420	29
Gambar 4.6 Upgrade Software OpenWRT.....	29
Gambar 4.7 Login OpenWRT.....	30
Gambar 4.8 Menu OpenWRT	31
Gambar 4.9 Network WIFI.....	31
Gambar 4.10 Join Network	32
Gambar 4.11 Network Join.....	32
Gambar 4.12 Network Koneksi	33
Gambar 4.13 PuTTY Configuration	33
Gambar 4.14 Interface Putty	34
Gambar 4.15 Update Template OpenWRT.....	35
Gambar 4.16 Opkg Install.....	35
Gambar 4.17 Cd /etc/freeradius2/.....	36
Gambar 4.18 Vi User.....	36

Gambar 4.19 Modify Line Text 76	37
Gambar 4.20 Konfigurasi Vi Clients	37
Gambar 4.21 Modify Line Text 34 Setting IP	38
Gambar 4.22 Setting Password.....	38
Gambar 4.23 Konfigurasi Vi Radiusd.....	39
Gambar 4.24 Modify Line Text 293	39
Gambar 4.25 Modify Line Text 443 Setting Perintah Auth.....	40
Gambar 4.26 Install Openssl-util	40
Gambar 4.27 Konfigurasi CDCerts.....	41
Gambar 4.28 Konfigurasi rm ca.pem.....	41
Gambar 4.29 Konfigurasi rm server.pem.....	42
Gambar 4.30 Konfigurasi Openssl Key	42
Gambar 4.31 Penambahan Password ca.key.....	43
Gambar 4.32 Setting Openssl req.....	43
Gambar 4.33 Setting Password certs.....	44
Gambar 4.34 Setting Openssl genrsa	44
Gambar 4.35 Input Password server.key.....	45
Gambar 4.36 Setting Openssl req –new	45
Gambar 4.37 Setting Password Optional Company.....	46
Gambar 4.38 Setting Openssl x509.....	46
Gambar 4.39 Konfigurasi Vi Eap.....	47

Gambar 4.40 Modify Line Text 158.....	47
Gambar 4.41 Modify Line Text 159	48
Gambar 4.42Review Status ps-A	48
Gambar 4.43 Start Radiusd	49
Gambar 4.44Review Status ps-A	49
Gambar 4.45Setting Interface Configuration.....	50
Gambar 4.46 WAP2-EAP	50
Gambar 4.47Setting WPA2-EAP.....	51
Gambar 4.48Setting Radiusd	51
Gambar 4.49Setting Network Windows	52
Gambar 4.50Setting Manually Connect to a Wireless Network.....	52
Gambar 4.51 Setting Change Connection Settings.....	53
Gambar 4.52Setting Remember My Credential for this Connection.....	53
Gambar 4.53Setting Radio Button Enable Pairwise Master Key (PMK)	54
Gambar 4.54Setting Protected EAP Properties.....	54
Gambar 4.55Setting EAP MSCHAPv2 Properties	55
Gambar 4.56Jaringan Freeradius	55
Gambar 4.57Interface Network Authentication.....	56
Gambar 4.58 Sukses Akses Jaringan Freeradius.....	56
Gambar 4.59 Login Internet.....	57
Gambar 4.60 Mac Address.....	57

Gambar 4.61 Interface Technetium.....	58
Gambar 4.62Change Mac Address	58
Gambar 4.63 Sukses Akses Jaringan dengan MACAddress berbeda.....	59
Gambar 4.64 Capture Data.....	59
Gambar 4.65 Interface LOIC	61
Gambar 4.66 Capture Sukses Requested DDOS Attack.....	61
Gambar 4.67 Capture Sukses DOS Attack	62
Gambar 4.68 Ip Address Awal.....	62
Gambar 4.69 Proxy	63
Gambar 4.70 Change IP Address.....	63
Gambar 4.71Akses Jaringan Internet.....	64
Gambar 4.72 Login Internet Radius Server.....	64
Gambar 4.73 Mac Address.....	65
Gambar 4.74 Interface Technetium.....	65
Gambar 4.75 Autentifikasi Ulang	66
Gambar 4.76 Capture Data.....	66
Gambar 4.77 Interface LOIC.....	68
Gambar 4.78 Capture Requested DDOS.....	68
Gambar 4.79 Capture Failed DOS Attac.....	69
Gambar 4.80 Ip Address Awal.....	70
Gambar 4.81 Proxy	70

Gambar 4.82Error Akses Jaringan	71
---------------------------------------	----

