



**PENGAMANAN JARINGAN *WIRELESS* LAN DENGAN  
MENGUNAKAN *AUTHENTICATION, AUTHORIZATION,  
ACCOUNTING* (AAA) DALAM MENCEGAH SERANGAN  
*RANDOM MAC ADDRESS***

**SKRIPSI**

**ARIANSYAH ARIFIN**

**1910511020**

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA  
FAKULTAS ILMU KOMPUTER  
PROGRAM STUDI S1 INFORMATIKA  
2023**



**PENGAMANAN JARINGAN *WIRELESS* LAN DENGAN  
MENGUNAKAN *AUTHENTICATION, AUTHORIZATION,  
ACCOUNTING* (AAA) DALAM MENCEGAH SERANGAN  
*RANDOM MAC ADDRESS***

**SKRIPSI**

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana  
Komputer**

**ARIANSYAH ARIFIN**

**1910511020**

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA  
FAKULTAS ILMU KOMPUTER  
PROGRAM STUDI S1 INFORMATIKA  
2023**

## PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Ariansyah Arifin

NIM : 1910511020

Tanggal : 17 Juli 2023

Judul Skripsi : **PENGAMANAN JARINGAN *WIRELESS* LAN DENGAN MENGGUNAKAN *AUTHENTICATION, AUTHORIZATION, ACCOUNTING* (AAA) DALAM MENCEGAH SERANGAN *RANDOM MAC ADDRESS***

Bilamana pada kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 17 Juli 2023

Yang Menyatakan,



Ariansyah Arifin

## SURAT PENYATAAN / PERSETUJUAN PUBLIKASI SKRIPSI

Sebagai civitas akademika Universitas Pembangunan Nasional "Veteran" Jakarta, saya yang bertandatangan dibawah ini :

Nama : Ariansyah Arifin  
NIM : 1910511020  
Fakultas : Ilmu Komputer  
Program Studi : S1 Informatika  
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui skripsi saya untuk di publikasikan bersama Dosen Pembimbing dengan keterangan sebagai berikut:

Judul Skripsi : Pengamanan Jaringan *Wireless* LAN Dengan Menggunakan *Authentication, Authorization, Accounting (AAA)* Dalam Mencegah Serangan *Random MAC Address*

Dosen Pembimbing : Henki Bayu Seta, S.Kom., M.Ti  
NIDN : 0309118104

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta  
Pada tanggal : 5 Juni 2023



( Ariansyah Arifin )


## LEMBAR PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama : Ariansyah Arifin  
NIM : 1910511020  
Program Studi : S1 Informatika  
Judul Tugas Akhir : Pengamanan Jaringan *Wireless* LAN Dengan Menggunakan *Authentication, Authorization, Accounting* (AAA) Dalam Mencegah Serangan *Random MAC Address*


Telah berhasil dipertahankan dihadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

  
Jayanta, S.Kom., M.Si.  
Penguji I

  
Theresia Wati, S.Kom., MTI.  
Penguji II

  
Henki Bayu Seta, S.Kom., MTI  
Pembimbing

  
Dr. Ermatita, M.Kom.  
Dekan

  
Dr. Widya Cholij, M.I.T.  
Kepala Program Studi

Ditetapkan di : Jakarta  
Tanggal Ujian : 22 Juni 2023



**PENGAMANAN JARINGAN *WIRELESS* LAN DENGAN  
MENGUNAKAN *AUTHENTICATION, AUTHORIZATION,  
ACCOUNTING (AAA)* DALAM MENCEGAH SERANGAN *RANDOM  
MAC ADDRESS***

**Ariansyah Arifin**

**ABSTRAK**

*Wireless* LAN salah satu tipe jaringan yang paling banyak digunakan karena kemudahannya. Namun dalam penggunaan jaringan ini, sering kali muncul beberapa masalah. salah satunya adalah fitur di *end device* yaitu Random MAC Address. Pada beberapa perangkat *end device* baru, seperti android 10, 12, iOS 16, windows 10. Konfigurasi default atau tidak default di pengaturan jaringannya adalah ada *Random MAC Address*. Terkadang fitur ini membuat *Network administrator* kesulitan pada saat mengatur *user*, membuat *IP Address pool* cepat habis karena *MAC Address* yang dipergunakan *user* yaitu berubah-ubah. Apalagi bila mengimplementasikan beberapa fitur manajemen jaringan seperti *bandwidth management, firewall* dan lain-lain akan sulit. Tujuan dalam penelitian ini adalah membuat pengamanan *Wireless* LAN yang ditingkatkan dan manajemen jaringan untuk dapat mencegah serangan *Random MAC Address*. Dengan melakukan penerapan metode protokol keamanan *Authentication, Authorization, Accounting (AAA)*, serta dikombinasikan dengan metode protokol otentikasi EAP PEAP-MSCHAPv2. Dengan metode tersebut, hasil penelitian ini menunjukkan bahwa sistem keamanan baru (EAP-PEAP MSCHAPv2 (AAA)) memiliki tingkat kesulitan koneksi yang lebih tinggi, dengan nilai rata-rata sebesar 2,70 dibandingkan dengan sistem keamanan sebelumnya (WPA2-PSK) yang memiliki nilai rata-rata sebesar 2,21. Nilai rata-rata yang lebih tinggi mengindikasikan peningkatan ketahanan terhadap serangan, menunjukkan kemampuan sistem keamanan baru dalam mencegah serangan *Random MAC Address*. Dalam hal kecepatan akses website, sistem keamanan baru mencapai nilai rata-rata yang lebih tinggi dibandingkan dengan sistem sebelumnya pada berbagai website seperti YouTube, Leads UPN Veteran Jakarta, email Google, dan Speedtest by Ookla. Temuan penelitian mengungkap perbedaan signifikan dalam kemampuan antara WPA2-PSK dan EAP-PEAP MSCHAPv2 (AAA) dalam mencegah dampak serangan *Random MAC Address* dan menjaga kinerja jaringan. WPA2-PSK mengalami masalah serius ketika pengguna "*Forget WiFi*" dan menghubungkan kembali, yang mengakibatkan habisnya alamat IP dan pembatasan *bandwidth*. Sebaliknya, EAP-PEAP MSCHAPv2 (AAA) menunjukkan resistansi yang lebih baik terhadap serangan "*Forget WiFi*", Sistem ini menjaga ketersediaan alamat IP, menjaga kualitas layanan jaringan yang baik, dan membatasi akses yang tidak sah.

**Kata Kunci :** *Wireless* LAN, Perangkat *End device*, *Random MAC Address*, IP Address Pool, AAA, EAP-PEAP MSCHAPv2, WPA2-PSK.

**SECURITY OF WIRELESS LAN NETWORKS USING AUTHENTICATION,  
AUTHORIZATION, ACCOUNTING (AAA) IN PREVENTING RANDOM  
MAC ADDRESS ATTACKS**

**Ariansyah Arifin**

**ABSTRACT**

*Wireless LAN is one of the most widely used network types because of its convenience. But in the use of this network, problems often arise. one of them is a feature on the end device, namely the Random MAC Address. On some new end devices, such as Android 10, 12, iOS 16, Windows 10. The default or non-default configuration in the network settings is that there is a Random MAC Address. Sometimes this feature makes it difficult for network administrators to manage users, causing the IP address pool to run out quickly because the MAC address used by the user changes. Especially if implementing several network management features such as bandwidth management, firewalls and others will be difficult. The purpose of this research is to make enhanced Wireless LAN security and network management to be able to prevent Random MAC Address attacks. By implementing the Authentication, Authorization, Accounting (AAA) security protocol method, and combined with the PEAP-MSCHAPv2 EAP authentication protocol method. With this method, the results of this study indicate that the new security system (EAP-PEAP MSCHAPv2 (AAA)) has a higher connection difficulty level, with an average value of 2.70 compared to the previous security system (WPA2-PSK) which has the average value of 2.21. A higher average value indicates increased resistance to attacks, indicating the ability of the new security system to prevent Random MAC Address attacks. In terms of website access speed, the new security system achieves higher average scores compared to the previous system on various websites such as YouTube, Leads UPN Veteran Jakarta, Google email, and Speedtest by Ookla. The research findings reveal significant differences in capabilities between WPA2-PSK and EAP-PEAP MSCHAPv2 (AAA) in preventing the impact of Random MAC Address attacks and maintaining network performance. WPA2-PSK encountered a serious problem when users "Forget WiFi" and reconnected, resulting in exhausted IP addresses and bandwidth throttling. On the other hand, EAP-PEAP MSCHAPv2 (AAA) shows better resistance to "Forget WiFi" attacks. This system maintains IP address availability, maintains good quality of network service, and restricts unauthorized access.*

**Keywords** : *Wireless LAN, End device, Random MAC Address, AAA, EAP-PEAP MSCHAPv2, WPA2-PSK*

## KATA PENGANTAR

Puji syukur saya ucapkan kepada Allah SWT atas karunia dan ridha-Nya yang diberikan, sehingga skripsi tugas akhir dengan judul “Pengamanan Jaringan *Wireless LAN* Dengan Menggunakan *Authentication, Authorization, Accounting (AAA)* Dalam Mencegah Serangan *Random MAC Address*” dapat dikerjakan tepat dalam waktunya. Penulis ingin mengucapkan terima kasih banyak kepada:

1. Ibu Dr. Ermatita, M.Kom. Selaku Dekan Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.
2. Ibu Dr. Widya Cholil, M.I.T, selaku Ketua Program Studi Informatika Universitas Pembangunan Nasional Veteran Jakarta.
3. Bapak Henki Bayu Seta, S.Kom., MTI. selaku dosen pembimbing skripsi tugas akhir yang telah bersedia meluangkan waktunya dan memberi arahan.
4. Seluruh dosen dan pegawai Fakultas Ilmu Komputer.
5. Kedua orang tua serta keluarga yang terus mendoakan dan memberi dukungan dalam berbagai hal.
6. Orang terdekat penulis, teman – teman Informatika angkatan 2019 dan kerabat kerja yang sudah membantu dan memotivasi penulis untuk menyelesaikan skripsi tugas akhir ini.

Penulis menyadari masih banyak memiliki kekurangan dan masih jauh dari kata sempurna dalam penyusunan skripsi tugas akhir ini, sehingga penulis mengharapkan saran dan kritik yang bersifat membangun untuk penulis. Akhir kata penulis ucapkan terima kasih.

Kota Bekasi, 27 Mei 2023

Ariansyah Arifin



# DAFTAR ISI

Halaman

<b>LEMBAR ORISINALITAS .....</b>	<b>i</b>
<b>SURAT PERNYATAAN / PERSETUJUAN PUBLIKASI SKRIPSI.....</b>	<b>ii</b>
<b>LEMBAR PENGESAHAN.....</b>	<b>iii</b>
<b>ABSTRAK.....</b>	<b>iv</b>
<b>ABSTRACT.....</b>	<b>v</b>
<b>KATA PENGANTAR.....</b>	<b>vi</b>
<b>DAFTAR ISI .....</b>	<b>vii</b>
<b>DAFTAR GAMBAR.....</b>	<b>viii</b>
<b>DAFTAR TABEL .....</b>	<b>ix</b>
<b>DAFTAR LAMPIRAN .....</b>	<b>xv</b>
<b>BAB 1 PENDAHULUAN.....</b>	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	4
1.3 Tujuan Penelitian .....	4
1.4 Manfaat.....	5
1.5 Ruang Lingkup.....	5
1.6 Luaran Yang Diharapkan .....	6
1.7 Sistematika Penulisan.....	6
<b>BAB 2 TINJAUAN PUSTAKA .....</b>	<b>8</b>
2.1 Konsep Keamanan Jaringan .....	8
2.1.1 Ancaman .....	8
2.1.2 Kerentanan .....	9
2.2 <i>Wireless Local Area Network</i> (WLAN) .....	9
2.2.1 Mode <i>Wireless Local Area Network</i> (WLAN).....	10
2.2.2 Komponen <i>Wireless Local Area Network</i> (WLAN).....	11
2.2.3 Badan Standarisasi Perangkat Dan Teknologi Jaringan Internasional .....	13
2.2.4 Mekanisme <i>Wireless Local Area Network</i> (WLAN).....	15
2.3 Protokol <i>Authentication, Authorization, Accounting</i> (AAA) .....	16

2.3.1	Remote <i>Authentication Dial-In User Service</i> (RADIUS)..	17
2.4	Protokol Otentikasi.....	24
2.4.1	WPA 2 PSK.....	25
2.4.2	<i>Extensible Authentication Protocol</i> (EAP) .....	26
2.5	Metode <i>Extensible Authentication Protocol</i> (EAP) .....	28
2.5.1	EAP TLS .....	28
2.5.2	EAP TTLS.....	29
2.5.3	EAP PEAP.....	29
2.6	Protokol <i>Secure Socket Layer</i> (SSL) / <i>Transport Layer Security</i> (TLS).....	31
2.6.1	Arsitektur SSL.....	33
2.6.2	<i>Public Key Infrastructure</i> (PKI).....	34
2.6.3	Kriptografi <i>Public Key &amp; Private Key</i> .....	34
2.6.4	<i>Registration Authority</i> .....	34
2.6.5	<i>Certificate Authority</i> .....	35
2.6.6	Sertifikat Digital .....	35
2.7	MAC Address .....	35
2.7.1	<i>Random MAC Address</i> .....	36
2.8	Perangkat <i>End device</i> .....	41
2.9	<i>User Manager v7</i> .....	41
2.10	Mikrotik.....	42
2.11	Bandwidth Alokasi.....	43
2.12	Penelitian Terkait .....	43
<b>BAB 3</b>	<b>METODE PENELITIAN.....</b>	<b>47</b>
3.1	Kerangka Pikir Penelitian .....	47
3.2	Metode Penelitian .....	48
3.2.1	Identifikasi Masalah.....	48
3.2.2	Pengumpulan Data.....	49
3.2.3	Tahapan Konfigurasi Sistem Keamanan Jaringan.....	49
3.2.4	Pengujian Sistem Keamanan Jaringan .....	53
3.2.5	Dokumentasi.....	54
3.3	Alat Bantu Penelitian .....	54

3.3.1. Alat bantu perangkat keras ( <i>Hardware</i> ) meliputi:.....	55
3.3.2. Alat bantu perangkat lunak ( <i>Software</i> ) meliputi: .....	56
3.4 Waktu Dan Tempat Penelitian.....	56
3.5 Jadwal Penelitian.....	56
<b>BAB 4 HASIL DAN PEMBAHASAN.....</b>	<b>58</b>
4.1 Pengumpulan Data .....	58
4.2 Analisa dan Pengujian Sistem Keamanan Sebelumnya .....	64
4.3 Implementasi Sistem Keamanan Yang Digunakan.....	82
4.3.1 Konfigurasi Basic Config Topologi.....	82
4.3.2 Konfigurasi Router Gateway <i>Authentication Server &amp;</i> <i>Accounting</i> ( <i>Radius Userman v7</i> ).....	83
4.3.3 Konfigurasi Access Point <i>Authenticator</i> .....	88
4.3.4 Konfigurasi Supplicant .....	89
4.3.5 Status <i>Session</i> Terkoneksi.....	90
4.4 Analisa dan Pengujian Sistem Keamanan Yang Digunakan .....	92
4.5 Perbandingan Kedua Keamanan .....	102
4.6 Analisa Hasil Kedua Keamanan Dalam Mencegah Serangan <i>Random Mac Address</i> .....	104
<b>BAB 5 SIMPULAN DAN SARAN .....</b>	<b>107</b>
5.1 Simpulan.....	107
5.2 Saran.....	108
<b>DAFTAR PUSTAKA.....</b>	<b>110</b>
<b>RIWAYAT HIDUP.....</b>	<b>113</b>
<b>LAMPIRAN.....</b>	<b>114</b>

## DAFTAR GAMBAR

Gambar 2.1.	Mode WLAN Ad Hoc .....	10
Gambar 2.2.	Mode WLAN Infrastructure .....	11
Gambar 2.3.	<i>Access Point</i> yang terhubung ke Jaringan .....	12
Gambar 2.4.	<i>Multiple Access Point</i> dengan <i>Roaming</i> .....	12
Gambar 2.5.	<i>Wireless Local Area Network Card</i> .....	13
Gambar 2.6.	Struktur paket RADIUS .....	18
Gambar 2.7.	Cara Kerja Koneksi RADIUS EAP .....	24
Gambar 2.8.	Arsitektur Protokol SSL .....	33
Gambar 2.9.	Mikrotik Routerboard 750Gr3 .....	43
Gambar 3.1.	Kerangka Pikir Penelitian .....	47
Gambar 3.2.	Penyederhanaan Topologi Jaringan pada lokasi <i>Wireless</i> saat ini. 50	
Gambar 3.3.	Rancangan Topologi Keamanan Jaringan Terbaru .....	50
Gambar 3.4.	<i>Flowchart</i> untuk konfigurasi sistem keamanan jaringan terbaru... 51	
Gambar 3.5.	<i>Flowchart</i> Pengujian sistem keamanan jaringan terbaru .....	54
Gambar 4.1.	Topologi Jaringan yang berjalan pada lokasi <i>Wireless</i> saat ini. ....	59
Gambar 4.5.	Bukti Indikasi Telah Terjadi serangan <i>Random MAC Address</i> Pada Jaringan <i>Wireless Local Area Network</i> hostpokit yang Berjalan. 62	
Gambar 4.6.	Bandwidth pada infrastruktur keamanan jaringan <i>Wireless</i> sebelumnya FIK-Hotspot.....	63
Gambar 4.7.	Pembuatan DHCP <i>Client</i> pada ether 1 yang arah menuju ISP .....	65
Gambar 4.8.	Pembuatan <i>Address</i> untuk memberikan IP <i>Address</i> LAN pada ether 5 ke Handphone/Laptop .....	65
Gambar 4.9.	Pembuatan DHCP <i>Server</i> untuk memberikan IP <i>Address</i> LAN pada ether 5 ke Handphone/Laptop.....	66
Gambar 4.10.	Pembuatan NAT untuk IP <i>Address</i> LAN pada ether 5 bisa akses ke internet.....	67
Gambar 4.11.	Pembuatan SSID ( <i>Service set identifier</i> ) untuk nama WiFi sistem keamanan jaringan sebelumnya dan keamanannya .....	68
Gambar 4.12.	Pembuatan bandwidth <i>profile</i> pada UniFi.....	68
Gambar 4.13.	Penambahan <i>settingan</i> bandwidth <i>profile</i> di wifi.....	69
Gambar 4.14.	Pengaturan pada iphone ios 16 saat mau terhubung ke jaringan ...	70
Gambar 4.15.	Pengaturan pada android versi 10 sampai dengan 13 saat mau terhubung ke jaringan.....	70
Gambar 4.16.	Pengaturan pada windows 10 serta 11 saat mau terhubung ke jaringan.....	71
Gambar 4.17.	Input <i>password</i> saat mau terhubung ke dalam jaringan .....	71
Gambar 4.18.	Perangkat berhasil terhubung ke dalam jaringan .....	71
Gambar 4.19.	38 Perangkat yang Terhubung ke dalam Jaringan Sistem Keamanan Sebelumnya Pada Sebelum Skenario Dijalankan Di Kelas Lab Pertama .....	72
Gambar 4.20.	39 Perangkat yang terhubung ke dalam jaringan sistem keamanan sebelumnya pada sebelum skenario dijalankan di kelas lab kedua	73

Gambar 4.21. Skenario <i>Random Mac Address</i> Dengan <i>forget</i> koneksi Wifi yang lagi terhubung lalu dikoneksikan ulang pada sistem keamanan sebelumnya .....	73
Gambar 4.22. Perangkat terhubung 61 dengan nyatanya perangkat cuman ada 38 <i>user</i> yang menempati dengan skenario sudah dijalankan pada kelas lab pertama .....	74
Gambar 4.23. Perangkat terhubung 61 dengan nyatanya perangkat cuman ada 39 <i>user</i> yang menempati dengan skenario sudah dijalankan pada kelas lab kedua.....	75
Gambar 4.24. Jaringan <i>down</i> karena IP DHCP sudah habis yang disebabkan oleh <i>Random MAC Address</i> .....	75
Gambar 4.25. Grafik Jenis Kelamin Responden <i>survey</i> penilaian pengujian sistem keamanan sebelumnya.....	76
Gambar 4.26. Grafik Usia Responden <i>survey</i> penilaian pengujian sistem keamanan sebelumnya .....	76
Gambar 4.27. Grafik perangkat yang digunakan saat melakukan koneksi ke WiFi_PenelitianWPA2PSK_ <i>RandomMac</i> .....	77
Gambar 4.28. Sistem operasi yang digunakan saat melakukan koneksi ke WiFi_PenelitianWPA2PSK_ <i>RandomMac</i> .....	77
Gambar 4.29. Perangkat Yang Digunakan Sudah Disetting Secara <i>Default</i> Aktif <i>Random MAC Address</i> Saat Mau Koneksi WiFi_PenelitianWPA2PSK_ <i>RandomMac</i> .....	78
Gambar 4.30. Grafik Tampilan Seberapa Mudah Tahapan Saat Melakukan Koneksi Ke WiFi_PenelitianWPA2PSK_ <i>RandomMac</i> .....	79
Gambar 4.31. Grafik Tampilan Seberapa Cepat Saat Melakukan Aktifitas Membuka Website Youtube pada <i>survey</i> penilaian pengujian sistem keamanan sebelumnya.....	79
Gambar 4.32. Grafik Tampilan Seberapa Cepat Saat Melakukan Aktifitas Membuka Website Leads UPN Veteran Jakarta pada <i>survey</i> penilaian pengujian sistem keamanan sebelumnya.....	80
Gambar 4.33. Grafik Tampilan Seberapa Cepat Saat Melakukan Aktifitas Membuka Website Email Google pada <i>survey</i> penilaian pengujian sistem keamanan sebelumnya .....	80
Gambar 4.34. Grafik Tampilan Seberapa Cepat Saat Melakukan Aktifitas Membuka Website Speedtest By Ookla pada <i>survey</i> penilaian pengujian sistem keamanan sebelumnya.....	81
Gambar 4.35. Tampilan <i>User Manager</i> versi 7 sudah terpasang dengan baik.....	83
Gambar 4.36. Tampilan SSL Sertifikat <i>Let's Encrypt</i> sukses dibuat.....	84
Gambar 4.37. Tampilan SSL Sertifikat <i>Let's Encrypt</i> Tersimpan dalam menu certificates mikrotik .....	84
Gambar 4.38. Tampilan pengaktifan dan pemasangan sertifikat SSL <i>User Manager</i> versi 7 di router utama.....	85
Gambar 4.39. Tampilan Konfigurasi Routres <i>User Manager</i> versi 7 di Router Utama .....	86

Gambar 4.40.	Tampilan Konfigurasi Radius <i>settings</i> pada Akses Point <i>Authenticator</i> .....	88
Gambar 4.41.	Tampilan konfigurasi buat wifi, security wifi dan pemilihan radius <i>profile</i> pada akses point <i>authenticator</i> .....	89
Gambar 4.42.	Tampilan konfigurasi <i>Wireless</i> access point pada akses point <i>authenticator</i> .....	89
Gambar 4.43.	Tampilan konfigurasi supplicant pada perangkat <i>end device</i> .....	90
Gambar 4.44.	Tampilan status <i>Session</i> terkoneksi di <i>User Manager</i> versi 7 .....	91
Gambar 4.45.	Tampilan status total uptime, <i>download</i> dan <i>upload</i> yang terkoneksi di <i>User Manager</i> versi 7.....	92
Gambar 4.46.	23 Perangkat yang terhubung ke dalam jaringan Sistem Keamanan terbaru pada sebelum skenario dijalankan di kelas lab pertama ....	93
Gambar 4.47.	27 Perangkat yang terhubung ke dalam jaringan Sistem Keamanan terbaru pada sebelum skenario dijalankan di kelas lab kedua .....	93
Gambar 4.48.	Skenario <i>Random Mac Address</i> Dengan <i>forget</i> koneksi Wifi yang lagi terhubung lalu dikoneksikan ulang pada sistem keamanan terbaru.....	94
Gambar 4.49.	Hasil pengujian sistem keamanan terbaru dengan skenario <i>forget</i> wifi sudah dijalankan pada kelas lab pertama .....	95
Gambar 4.50.	Hasil pengujian sistem keamanan terbaru dengan skenario <i>forget</i> wifi sudah dijalankan pada kelas lab kedua.....	95
Gambar 4.51.	Grafik Jenis Kelamin Responden <i>survey</i> penilaian pengujian sistem keamanan terbaru .....	96
Gambar 4.52.	Grafik Usia Responden <i>survey</i> penilaian pengujian sistem keamanan terbaru.....	97
Gambar 4.53.	Grafik perangkat yang digunakan saat melakukan koneksi ke WiFi_PenelitianWPAEAP_RandomMac.....	97
Gambar 4.54.	Sistem operasi yang digunakan saat melakukan koneksi ke WiFi_PenelitianWPAEAP_RandomMac.....	97
Gambar 4.55.	Perangkat Yang Digunakan Sudah Disetting Secara <i>Default</i> Aktif <i>Random MAC Address</i> Saat Mau Koneksi WiFi_PenelitianWPAEAP_RandomMac.....	98
Gambar 4.56.	Grafik Tampilan Seberapa Mudah Tahapan Saat Melakukan Koneksi Ke WiFi_PenelitianWPAEAP_RandomMac.....	99
Gambar 4.57.	Grafik Tampilan Seberapa Cepat Saat Melakukan Aktifitas Membuka Website Youtube pada <i>survey</i> penilaian pengujian sistem keamanan terbaru .....	100
Gambar 4.58.	Grafik Tampilan Seberapa Cepat Saat Melakukan Aktifitas Membuka Website Leads UPN Veteran Jakarta pada <i>survey</i> penilaian pengujian sistem keamanan terbaru .....	100
Gambar 4.59.	Grafik Tampilan Seberapa Cepat Saat Melakukan Aktifitas Membuka Website Email Google pada <i>survey</i> penilaian pengujian sistem keamanan terbaru .....	101

Gambar 4.60. Grafik Tampilan Seberapa Cepat Saat Melakukan Aktifitas Membuka Website Speedtest By Ookla pada *survey* penilaian pengujian sistem keamanan terbaru ..... 101

## DAFTAR TABEL

Tabel 2.1.	Kode Jenis pesan RADIUS.....	18
Tabel 2.2.	Paket <i>Access-Request</i> .....	20
Tabel 2.3.	Paket <i>Access-Challenge</i> .....	21
Tabel 2.4.	Paket <i>Access-Accept</i> .....	22
Tabel 2.5.	Paket <i>Access-Reject</i> .....	22
Tabel 2.6.	Perbandingan metode otentikasi dalam EAP untuk Wi-Fi.....	31
Tabel 2.7.	OS Yang Telah Menerapkan <i>Random MAC Address</i> .....	36
Tabel 2.8.	Model perilaku <i>action</i> serangan <i>random MAC address</i> pada setiap sistem operasi.....	38
Tabel 3.1.	Tabel Jadwal Periode Penelitian .....	57
Tabel 4.1	Nilai Rata-Rata Dari Penilaian Pengujian Sistem Keamanan Sebelumnya.....	81
Tabel 4.3	Perbandingan Nilai Rata-Rata Dari Penilaian Pengujian Sistem Keamanan Sebelumnya Dengan Yang Terbaru.....	103



## DAFTAR LAMPIRAN

Lampiran 1. Konfigurasi Basic Config Topologi Sistem Keamanan EAP-PEAP MSCHAPV2 (AAA) .....	114
Lampiran 2. Konfigurasi <i>Usermanager</i> Versi 7 Dan Manajemen Jaringan .....	117
Lampiran 3. Surat Izin Penelitian .....	125
Lampiran 4. Foto Saat Pengujian Pengamanan Jaringan <i>Wireless</i> LAN Dengan Menggunakan <i>Authentication, Authorization, Accounting</i> (AAA) Dalam Mencegah Serangan <i>Random MAC Address</i> . .....	127