

**ANALISIS KEAMANAN WPA2-PSK DAN RADIUS SERVER
MENGUNAKAN METODE WIRELESS PENETRATION TESTING**

TUGAS AKHIR



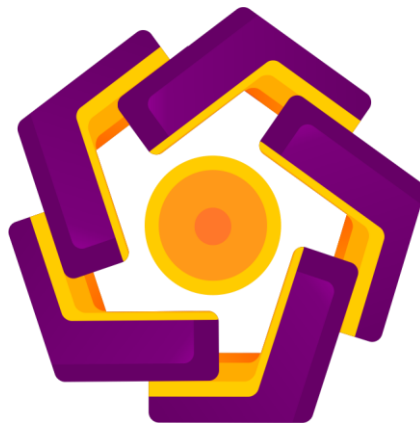
disusun oleh
Yusuf Vebrianto
16.11.0458

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
UNIVERSITAS AMIKOM YOGYAKARTA
2020**

**ANALISIS KEAMANAN WPA2-PSK DAN RADIUS SERVER
MENGUNAKAN METODE WIRELESS PENETRATION TESTING**

TUGAS AKHIR

untuk memenuhi sebagian persyaratan mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Yusuf Vebrianto

16.11.0458

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
UNIVERSITAS AMIKOM YOGYAKARTA
2020**

PERSETUJUAN

SKRIPSI

ANALISIS KEAMANAN WPA2-PSK DAN RADIUS SERVER MENGUNAKAN METODE WIRELESS PENETRATION TESTING

yang dipersiapkan dan disusun oleh

Yusuf Vebrianto

16.11.0458

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 30 Maret 2020

Dosen Pembimbing,

Heri Sismoro, M.Kom

NIK. 190302057

PENGESAHAN

SKRIPSI

ANALISIS KEAMANAN WPA2-PSK DAN RADIUS SERVER MENGUNAKAN METODE WIRELESS PENETRATION TESTING

yang dipersiapkan dan disusun oleh

Yusuf Vebrianto

16.11.0458

telah dipertahankan di depan Dewan Penguji
pada tanggal 17 April 2020

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Heri Sismoro, M.Kom
NIK. 190302057

Ferry Wahyu Wibowo, S.Si, M.Cs
NIK. 190302235

Agung Nugroho, M.Kom
NIK. 190302242

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 April 2020

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, 23 April 2020

Meterai
Rp. 6.000

Yusuf Vebrianto
NIM. 16.11.0458

MOTTO

You Cant Run But You Cant Hide

(Kardel Sharpeye)

Jangan menunda pekerjaan karena dapat berujung kepada kehancuran.

"Ya rabbku, lapangkanlah untukku dadaku, dan mudahkanlah untukku urusanku, dan lepaskanlah kekakuan dari lidahku, supaya mereka mengerti perkataanku. " (QS. Thaha (20) :25-28).

"Hidup itu seperti sepeda. Agar tetap seimbang, kau harus terus bergerak."

(Albert Einstein)

PERSEMBAHAN

Alhamdulillah rabbil'alamin puji syukur atas kehadiran Allah SWT berkat rahmat dan karunia-Nya lah penulis dapat menyelesaikan skripsi ini sebagai salah satu persyaratan untuk mencapai gelar Sarjana Komputer. Skripsi ini saya persembahkan kepada :

1. Kedua Orang Tua, Bapak Puguh, S.Pd.I dan Ibu Mistun serta seluruh keluarga besar yang senantiasa memberikan semangat, doa, serta motivasi yang tiada henti.
2. Bapak Heri Sismoro, M.Kom, selaku dosen pembimbing yang selalu mengarahkan dan memberikan masukan dalam proses penyusunan skripsi ini.
3. Seluruh dosen dan staff Universitas Amikom Yogyakarta yang telah memberikan ilmu dan pengalaman yang luar biasa.
4. Teman – teman kelas 16-S1IF-07 atas kebersamaan selama kuliah di Universitas Amikom Yogyakarta.
5. Terimakasih kepada Ferdina Anissariswari selaku teman seperjuangan dari masuk kuliah hingga lulus di Universitas Amikom Yogyakarta.
6. Terimakasih kepada partner hidup Ilva Indriani yang telah mensupport saya dalam menyelesaikan skripsi ini, dan semoga langgeng
7. Terimakasih kepada sahabat saya Basir, Lingga, Fikri, Ririn, Farid, teman kontraan biru, yang selalu memberi suport ejekan dan semangatnya untuk menyelesaikan skripsi ini.

KATA PENGANTAR

Assalamu'alaikum warahmatullahi wabarakatuh

Bismillahirrahmannirrohim

Puji dan Syukur Penulis panjatkan kehadiran Allah SWT. Karena atas limpahan Berkah dan Karunia nya saya dapat menyelesaikan skripsi ini. Shalawat serta salam tidak lupa saya junjungkan kepada nabi kita Muhammad SAW. Semoga kita diberi syafaatnya. Amin.

Tujuan Penulisan ini adalah salah satu syarat untuk menyelesaikan program Sarjana Satu di Universitas Amikom Yogyakarta, Oleh karena itu, penulis menyampaikan rasa terima kasih kepada :

1. Bapak Heri Sismoro, M.Kom selaku dosen pembimbing.
2. Prof. Dr. M. Suyanto, MM selaku Rektor Universitas Amikom Yogyakarta yang telah memberikan kesempatan kepada penulis untuk menimba ilmu di kampus ini.
3. Seluruh dosen dan staff Universitas Amikom Yogyakarta.
4. Orang tua dan keluarga yang telah memberikan dukungan baik secara moril maupun materiil.
5. Teman-teman seperjuangan yang selalu membantu dalam penyusunan skripsi ini.

Penulis menyadari bahwa penulisan Skripsi ini masih jauh dari sempurna. Keterbatasan kemampuan dan pengetahuan penulis merupakan faktor utama dari ketidaksempurnaan ini. Oleh karena itu, saran dan kritik yang sifatnya membangun sangat diharapkan oleh penulis. Semoga skripsi ini dapat bermanfaat dan dikembangkan untuk kepentingan lebih lanjut.

Yogyakarta, 27 April 2020

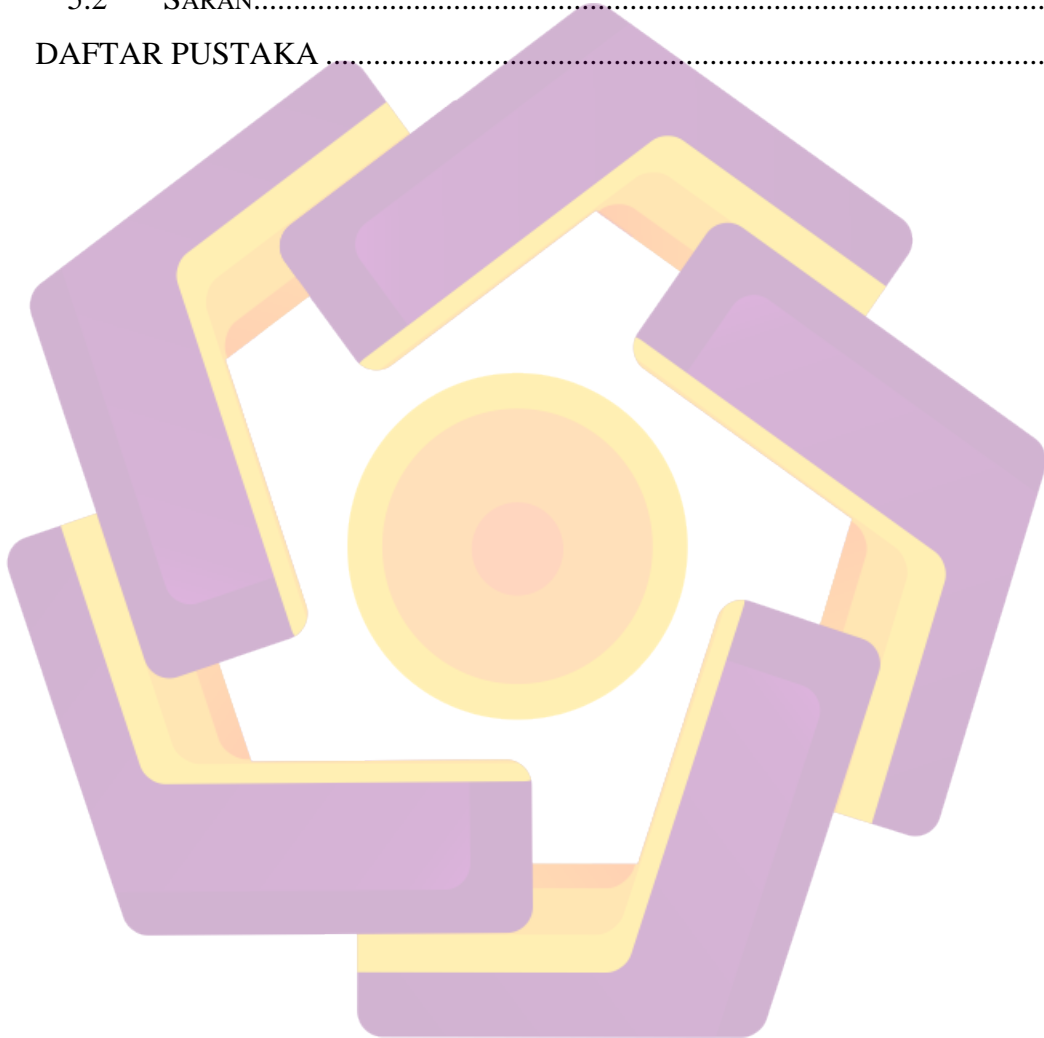
Penulis

DAFTAR ISI

DAFTAR ISI.....	II
DAFTAR TABEL.....	V
DAFTAR GAMBAR	VI
BAB I PENDAHULUAN.....	1
1.1 LATAR BELAKANG.....	1
1.2 RUMUSAN MASALAH.....	2
1.3 BATASAN MASALAH.....	2
1.4 MAKSUD DAN TUJUAN PENELITIAN.....	3
1.4.1 MAKSUD	3
1.4.2 TUJUAN	3
1.5 MANFAAT PENELITIAN.....	4
1.6 METODE PENELITIAN	4
1.6.1 METODE PENETRATION TESTING	4
1.7 SISTEMATIKA PENULISAN	6
BAB II LANDASAN TEORI.....	8
2.1 KAJIAN PUSTAKA.....	8
2.2 LANDASAN TEORI	11
2.2.1 PENGERTIAN JARINGAN KOMPTER.....	11
2.2.2 PENGERTIAN WIFI	15
2.2.3 PENGERTIAN MIKROTIK.....	17
2.2.3.1 JENIS MIKROTIK	17
2.2.3.2 PENGERTIN RADIUS MIKROTIK	18
2.2.4 CAPTIVE PORTAL	18
2.2.5 PENGERTIAN RADIUS	19
2.2.6 PROTOKOL RADIUS SERVER.....	20
2.2.7 PROSES AAA PADA RADIUS.....	21
2.2.8 WI-FI PROTECTED ACCESS PRE-SHARE (WPA2-PSK).....	22
2.3 METODE PENELTIAN	23

2.3.1	METODE PENETRATION TESTING	23
2.3.2	KONSEP METODE PENETRATIO TESTING.....	23
BAB III	IDENTIFIKASI DAN ANALISIS	25
3.1	INTELLIGENCE GATHERING.....	25
3.1.1	KEBUTUHAN PERANGKAT KERAS	25
3.1.2	KEBUTUHAN PERANGKAT LUNAK.....	27
3.2	ALUR PENELITIAN.....	28
3.2.1	ALUR PENELITIAN PENETRITION TESTING.....	28
3.2.2	GAMBARAN RANCANGAN PENGUJIAN.....	29
3.3	VULNERABILITY ANALYSIS.....	30
3.3.1	IDENTIFIKASI CELAH KEAMANAN WPA2-PSK.....	30
3.3.2	IDENTIFIKASI CELAH KEAMANAN RADIUS SERVER.....	32
3.4	MENENTUKAN JENIS SERANGAN/THREAT MODELING	35
3.4.1	SERANGAN BRUTE FORCE	35
3.4.2	MAC ADDRESS SPOOFING	35
3.4.3	SNIFFING TO EAVESDROP	36
3.4.4	MAN IN THE MIDDLE ATTACK	36
3.4.5	PING OF DEATH (POD).....	37
BAB IV	PENGUJIAN DAN HASIL.....	38
4.1	PASSWORD CRACKING.....	38
4.1.1	PENGUJIAN MENGGUNAKAN BRUTE FORCE	38
4.1.1.1	BRUTE FORCE WPA2-PSK.....	38
4.1.1.2	BRUTE FORCE RADIUS SERVER CAPTIVE PORTAL.....	43
4.1.2	PENGUJIAN MAC ADDRESS SPOOFING DENGAN MACCHANGER ...	44
4.1.2.1	MAC ADDRESS SPOOFING WAP2-PSK.....	44
4.1.2.2	MAC ADDRESS SPOOFING RADIUS SERVER.....	47
4.1.3	PENGUJIAN MENGGUNAKAN SNIFFING TO EAVASDROP.....	50
4.1.3.1	SNIFFING TO EAVESDROP WPA2-PSK	50
4.1.3.2	SNIFFING TO EAVESDROP RADIUS SERVER	52
4.1.4	PENGUJIAN MENGGUNAKAN PING OF DEATH.....	53
4.1.5	PENGUJIAN MENGGUNAKAN MAIN IN THE MIDLE.....	55

4.1.5.1 MAN IN THE MIDLE WPA2-PSK	55
4.1.5.2 MAIN IN THE MIDLE RADIUS SERVER CAPRIVE PORTAL .	57
4.2 HASIL PENGUJIAN DAN PEMBAHASAN	59
BAB V PENUTUP.....	61
5.1 KESIMPULAN.....	61
5.2 SARAN.....	63
DAFTAR PUSTAKA	64



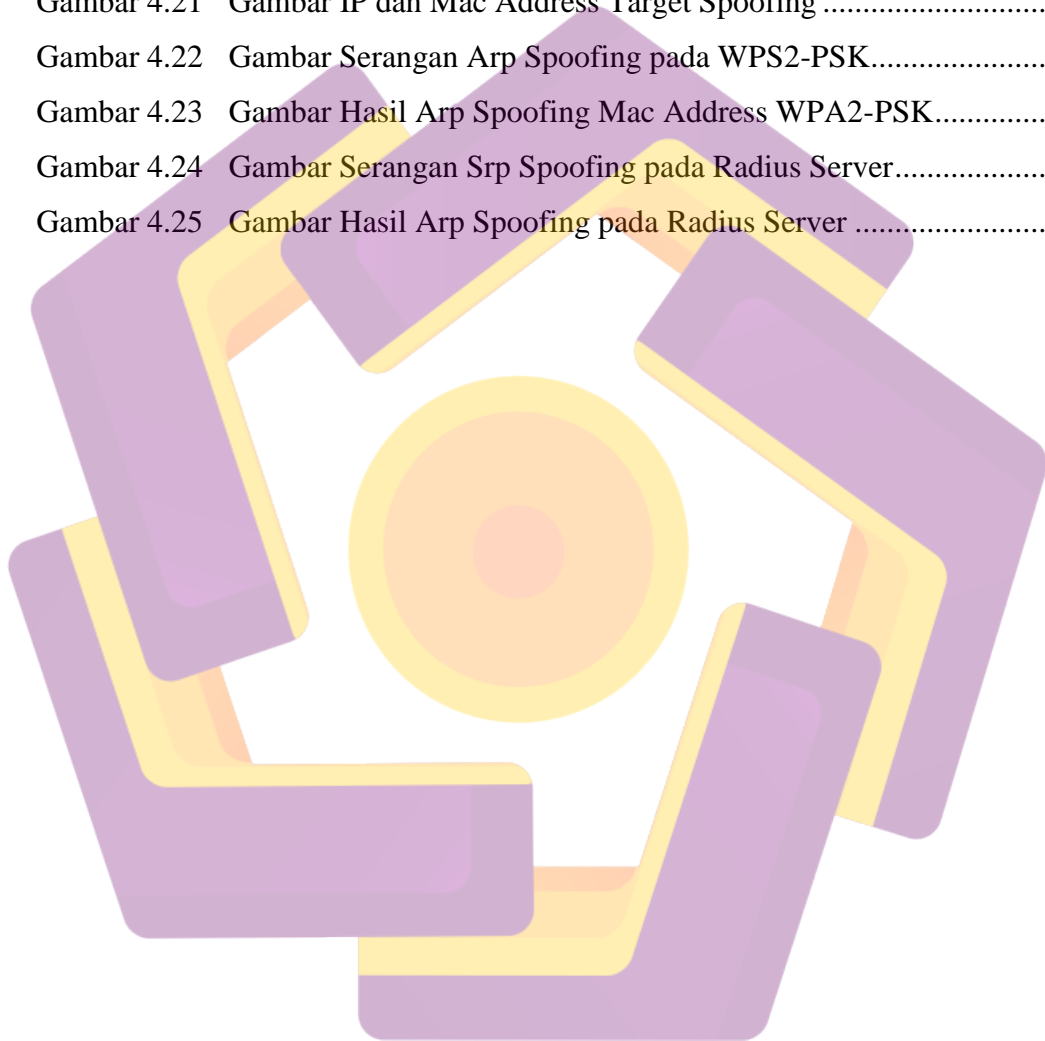
DAFTAR TABEL

Tabel 2.1	Perbandingan dengan Jeki Supriyanto	8
Tabel 2.2	Perbandingan dengan Penelitian Surahmat, Yesi N, Deny E	9
Tabel 2.3	Perbandingan dengan Gede Arna S, I Putu Oktap I, Putu	10
Tabel 2.4	Perbandingan dengan Erfan W, Emha Taufiq L, M Masjun E	11
Tabel 3.1	Spesifikasi Laptop	25
Tabel 3.2	Spesifikasi Roter Mikrotik	26
Tabel 3.3	<i>Operating System</i>	26
Tabel 3.4	Aplikasi dan <i>Tool</i> yang digunakan	27
Tabel 4.1	Mac Address Spoofing WPA2-PSK	46
Tabel 4.2	Mac Address Spoofing Radius Server dengan Captive Portal	48
Tabel 4.3	Tabel IP dan MAC target Arp Spoofing	55
Tabel 4.4	Tabel Hasil Pengujian	59

DAFTAR GAMBAR

Gambar 2.1	Gambar jaringan LAN.....	14
Gambar 2.2	Jaringan WLAN	14
Gambar 2.3	Jaringan MAN.....	15
Gambar 2.4	Contoh Jaringan WIFI.....	16
Gambar 2.5	Contoh gambar Captive Portal	19
Gambar 2.6	Flowchart metode Penetration Testing.....	23
Gambar 3.1	Diagram alur <i>Penetration Testing</i>	28
Gambar 3.2	Gambar Rancangan Pengujian	29
Gambar 3.3	Gambar Settingan WPA2-PSK	30
Gambar 3.4	Gambar Hasil Scan <i>Aircrack-ng</i> WP2-PSK.....	31
Gambar 3.5	Gambar Tampilan Menu Nessus Versi 7	32
Gambar 3.6	Gambar Settingan IP Address Target pada Nessus.....	33
Gambar 3.7	Gambar Hasil Scan Kerentanan Tingkat Tinggi	34
Gambar 3.8	Gambar Hasil Scan Radius Server dengan Nessus	34
Gambar 4.1	Interfaces yang Terhubung dengan WIFI	38
Gambar 4.2	Nama Antar Muka Monitor pada Interfaces	39
Gambar 4.3	Nama Bssid dan Mac Address Scan.....	40
Gambar 4.4	BSSID dan Client yang Terhubung	40
Gambar 4.5	Pengiriman Paket Deauthentication.....	41
Gambar 4.6	File Handshake Extentions .cap	41
Gambar 4.7	Hasil Crack Pasword WPA2-PSK	42
Gambar 4.8	Hasil <i>Brute Force Radius Server</i>	43
Gambar 4.9	Interfaces yang Terhubung dengan WLAN	44
Gambar 4.10	Interfaces Yang di Nonaktifkan	45
Gambar 4.11	Bahasa dan Fungsi Fungsi dari Macchanger.....	45
Gambar 4.12	<i>Mac Address</i> Permanent dan Manipulasi WPA2.....	46
Gambar 4.13	Hasil Pengujian <i>Mac Address Spoofing</i> WPA2.....	47
Gambar 4.14	<i>Mac Address</i> Permanen dan Manipulasi Radius.....	48
Gambar 4.15	Hasil <i>Mac Address Spoofing</i> Pada <i>Captive Portal</i>	49

Gambar 4.16	Filter Protokol HTTP Wireshark.....	50
Gambar 4.17	Aktifitas Client Untuk Pengujian.....	51
Gambar 4.18	Hasil Scan Wirshark Client.....	52
Gambar 4.19	Hasil Scan Wireshark pada Radius Server.....	53
Gambar 4.20	Gambar <i>Ping of Death</i> pada WPA2-PSK	54
Gambar 4.21	Gambar IP dan Mac Address Target Spoofing	56
Gambar 4.22	Gambar Serangan Arp Spoofing pada WPS2-PSK.....	56
Gambar 4.23	Gambar Hasil Arp Spoofing Mac Address WPA2-PSK.....	57
Gambar 4.24	Gambar Serangan Srp Spoofing pada Radius Server.....	58
Gambar 4.25	Gambar Hasil Arp Spoofing pada Radius Server	58



INTISARI

Wireless adalah suatu jaringan LAN (*Local Area Network*) nirkabel (*Wireless LAN*) yang tersedia untuk publik di suatu lokasi untuk megakses internet. Dalam penggunaanya *Wireless* juga memiliki sistem keamanan yang ada didalamnya seperti WPA2-PSK dan Radius Server.

Banyaknya perusahaan maupun individu yang mengimplementasikan jaringan nirkabel ini tak lepas dari permasalahan yang paling sering dijumpai dalam telekomunikasi, yaitu masalah keamanan. Banyak orang yang masih ragu akan kemanan jaringan wireless, dan banyak pula yang menyakini bahwa sistem kemanan *Wireless* yang menggunakan WPA2-PSK lebih aman dibandingkan dengan sistem keamanan wireless yang lain. Namun hasil study pustaka yang dilakukan, sistem keamanan *Wireless* yang benar benar mampu memberikan keamanan yang lebih source adalah dengan menggunakan sistem kemanan RADIUS Server.

Tujuan dari penelitian yang dilakukan adalah melakukan analisis sistem keamanan WPA2-PSK dengan RADIUS Server Mikrotik dan mendapatkan hasilnya untuk mengetahui sistem keamanan yang lebih aman. Pengujian dilakukan dengan menggunakan metode *Wireless Penetration Testing* dengan melakukan beberapa kemungkinan serangan seperti *Brute Force*, *MAC Address Spoofing*, *Snifing to Eavesdrop*, *MiTm*, dan *Ping Of Death*.

Kata Kunci: RADIUS, WPA2-PSK, Penetration Testing, Captive Portal

ABSTRACT

Wireless is an LAN network (Local Area Network) nirkabel (LAN *Wireless*) which available to public in an location to access internet. In its him *Wireless* also have security system exist in depth like WPA2-PSK and Radius Server.

The number of companies and individuals who implement this wireless network cannot be separated from the problems most often encountered in telecommunications is a security problem. Many people are still unsure of *Wireless* security, and many believe that wireless security system using WPA2-PSK are more secure than other *Wireless* security system. However, from the result of literature studies conducted, the *Wireless* security system that rally can provide more secure security is to use the security RADIUS Server.

The purpose of research is analyzing the WPA2-PSK with RADIUS Server mikrotik an get the results to find out the security system a more secure. Testing is done using *Wireless* penetration testing method by performing several possible attacks such as *Brute Force*, *MAC Address Spoofing*, *Sniffing to Eavesdrop*, *MiTM*, and *Ping Of Death*.

Keywords: RADIUS, WPA2-PSK, Penetration Testing, Captive Portal.