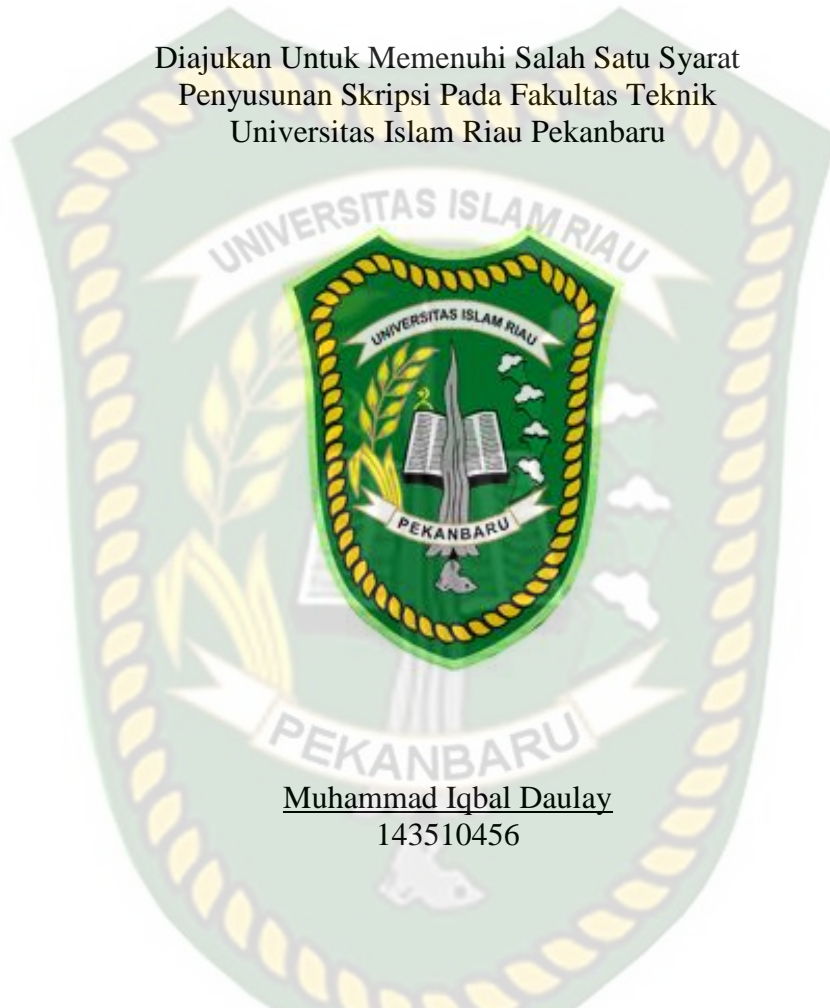


Analisis Perbandingan Keamanan WEP, WPA, WPA2, Pada Access Point

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat
Penyusunan Skripsi Pada Fakultas Teknik
Universitas Islam Riau Pekanbaru



Muhammad Iqbal Daulay
143510456

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM RIAU
PEKANBARU
2019

ANALISIS PERBANDINGAN KEAMANAN WEP, WPA, WPA2, PADA ACCESS POINT

MUHAMMAD IQBAL DAULAY
Fakultas Teknik
Program Studi Teknik Informatika
Universitas Islam Riau
E-mail : m.iqbaldaulay@student.uir.ac.id

Abstrak

Pada saat ini keamanan jaringan sangat rentan, maka keamanan jaringan ini bermula memakai keamanan *WEP* yang pertama kali rilis atau keluar dipakai oleh *client*. Setelah itu karna keamanan *WEP* ini mudah diretas oleh pihak yang tidak bertanggung jawab, maka adanya versi untuk keamanan yang lebih baik dari keamanan *WEP* keluarlah keamanan *WPA-PSK* dengan keamanan yang lebih unggul dari keamanan sebelumnya yaitu *WEP*. Lalu dengan berjalannya keamanan *WPA-PSK* ini masih ada juga celah untuk meretas keamanan *WPA-PSK* tersebut. Maka rilis lah kemanan yang sangat unggul dari kedua keamanan tersebut yaitu *WPA2-PSK*. Adapun simulasi untuk menilai dan mengukur tingkat keamanan tersebut adalah “ Analisis Perbandingan Keamanan WEP, WPA, WPA2, Pada Access Point “.

Kata Kunci : *WEP, WPA, WPA2, Perbandingan*

ANALYSIS OF SECURITY COMPARISON OF WEP, WPA, WPA2, ON THE ACCESS POINT

MUHAMMAD IQBAL DAULAY
Departement Of Informatics Engineering
Islamic University Of Riau
Email : m.iqbaldaulay@student.uir.ac.id

Abstract

At this time, network security is very vulnerable, then this network security started using WEP security which was first released or used by the client. After that, because the WEP security was easily be hacked by irresponsible parties, then there was a version for better security from WEP security, coming out WPA-PSK security with security that was more superior from the previous security, namely WEP. The over time the security of the WPA-PSK there was still a gap to hack the security of the WPA-PSK. Then released a security that was very superior from the two securities, namely was WPA2-PSK. At this time, the security requires an attention seriously because this is one of the important factor in building a network in order to know the technical weaknesses point in network connections. And as for the purpose to compare the level of security in WEP, WPA, WPA2, the results were to finding out which was more feasible or stronger security levels in the WEP, WPA, WPA2 methods.

The simulation was to assess and regulate the level of security was " The security comparative analysis of WEP, WPA, WPA2, on the access point",

Keyword : *WEP, WPA, WPA2, Comparison*

DAFTAR ISI

HALAMAN JUDUL

LEMBAR PERNYATAAN BEBAS PLAGIARISME

LEMBAR IDENTITAS PENULIS

HALAMAN PERSEMBAHAN

KATA PENGANTAR..... i

ABSTRAK iii

ABSTRACK iv

DAFTAR ISI..... v

DAFTAR TABEL vii

DAFTAR GAMBAR..... viii

BAB I PENDAHULUAN

1.1 Latar Belakang 1

1.2 Identifikasi Masalah 3

1.3 Batasan Masalah..... 3

1.4 Rumusan Masalah 3

1.5 Tujuan Penelitian 3

1.6 Manfaat Penelitian 4

BAB II LANDASAN TEORI

2.1 Studi Kepustakaan..... 5

2.2 Dasar Teori 7

2.2.1 WEP 7

2.2.2 WPA-PSK 8

2.2.3 WPA2-PSK 8

2.2.4 Perbedaan Keamanan WEP, WPA, WPA2 9

2.2.4.1 WEP.....9

2.2.4.2 WPA-PSK.....10

2.2.4.3 WPA2-PSK.....11

2.2.5 Acces Point12

2.2.6 Aircrack.....	13
2.2.6.1 Fungsi Aircrack-ng.....	13
2.2.7 Flowchart	14
BAB III METODOLOGI PENELITIAN	
3.1 Alat dan Bahan Penelitian	16
3.1.1 Spesifikasi Perangkat Keras	17
3.1.2 Spesifikasi Perangkat Lunak	17
3.2 Metode Penelitian.....	18
3.3 Jenis Data	19
3.4 Metode Pengumpulan Data	20
3.5 Pengembangan dan perancangan Sistem.....	21
3.5.1 Desain Topologi	21
3.5.5.1 Topologi Physical LAB IT.....	21
3.5.5.2 Topologi Logical LAB IT	22
3.6 Simulasi Serangan Terhadap WEP, WPA-PSK dan WPA2-PSK. 24	
3.6.1 Rancangan Serangan	24
3.6.2 Serangan Terhadap WPA-PSK dan WPA2-PSK.....	26
3.7 Flowchart Serangan WEP, WPA-PSK dan WPA2-PSK	26
3.8 Rancangan Proses Pengujian Keamanan Jaringan	27
BAB IV HASIL DAN PEMBAHASAN	
4.1 Melakukan Konfigurasi Pada Access Point	29
4.2 Hasil Akhir Pengujian Metode WEP	29
4.3 Hasil Akhir Pengujian Metode WPA-PSK	35
4.4 Hasil Akhir Pengujian Metode WPA2-PSK	46
BAB V KESIMPULAN DAN SARAN	
5.1 Kesimpulan	59
5.2 Saran.....	59
DAFTAR PUSTAKA	

DAFTAR TABEL

Tabel 2.1 Simbol dan fungsi flowchart	14
Tabel 3.1 Perangkat Keras.....	17
Tabel 3.2 Perangkat Lunak.....	18



DAFTAR GAMBAR

Gambar 3.1	Skema Prosedur Penelitian	21
Gambar 3.2	Rancangan Topologi Physical Lab IT	23
Gambar 3.3	Rancangan Topologi Logical Lab IT	24
Gambar 3.4	Simulasi Serangan Terhadap Wep, Wpa dan Wpa2	25
Gambar 3.5	Flochart Serangan WEP, WPA dan WPA2	27
Gambar 3.6	Monitoring Jaringan yang Terdeteksi	28
Gambar 3.7	Hasil Akhir Pengujian	28
Gambar 4.1	Hasil Akhir Pengujian Ke 1.....	29
Gambar 4.2	Hasil Akhir Pengujian Ke 2.....	30
Gambar 4.3	Hasil Akhir Pengujian Ke 3.....	30
Gambar 4.4	Hasil Akhir Pengujian Ke 4.....	31
Gambar 4.5	Hasil Akhir Pengujian Ke 5.....	31
Gambar 4.6	Hasil Akhir Pengujian Ke 6.....	31
Gambar 4.7	Hasil Akhir Pengujian Ke 7.....	32
Gambar 4.8	Hasil Akhir Pengujian Ke 8.....	32
Gambar 4.9	Hasil Akhir Pengujian Ke 9.....	32
Gambar 4.10	Hasil Akhir Pengujian Ke 10.....	33
Gambar 4.11	Hasil Akhir Pengujian Ke 11.....	33
Gambar 4.12	Hasil Akhir Pengujian Ke 12.....	33
Gambar 4.13	Hasil Akhir Pengujian Ke 13.....	34
Gambar 4.14	Hasil Akhir Pengujian Ke 14.....	34

Gambar 4.15 Hasil Akhir Pengujian Ke 15.....	34
Gambar 4.16 Hasil Akhir Pengujian Ke 16.....	35
Gambar 4.17 Hasil Akhir Pengujian Ke 1.....	35
Gambar 4.18 Hasil Akhir Pengujian Ke 2.....	36
Gambar 4.19 Hasil Akhir Pengujian Ke 3.....	36
Gambar 4.20 Hasil Akhir Pengujian Ke 4.....	37
Gambar 4.21 Hasil Akhir Pengujian Ke 5.....	37
Gambar 4.22 Hasil Akhir Pengujian Ke 6.....	38
Gambar 4.23 Hasil Akhir Pengujian Ke 7.....	38
Gambar 4.24 Hasil Akhir Pengujian Ke 8.....	39
Gambar 4.25 Hasil Akhir Pengujian Ke 9.....	39
Gambar 4.26 Hasil Akhir Pengujian Ke 10.....	40
Gambar 4.27 Hasil Akhir Pengujian Ke 11.....	40
Gambar 4.28 Hasil Akhir Pengujian Ke 12.....	41
Gambar 4.29 Hasil Akhir Pengujian Ke 13.....	41
Gambar 4.30 Hasil Akhir Pengujian Ke 14.....	42
Gambar 4.31 Hasil Akhir Pengujian Ke 15.....	42
Gambar 4.32 Hasil Akhir Pengujian Ke 16.....	43
Gambar 4.33 Hasil Akhir Pengujian Ke 17.....	43
Gambar 4.34 Hasil Akhir Pengujian Ke 18.....	44
Gambar 4.35 Hasil Akhir Pengujian Ke 19.....	44
Gambar 4.36 Hasil Akhir Pengujian Ke 20.....	45
Gambar 4.37 Hasil Akhir Pengujian Ke 21.....	45

Gambar 4.38 Hasil Akhir Pengujian Ke 1.....	46
Gambar 4.39 Hasil Akhir Pengujian Ke 2.....	46
Gambar 4.40 Hasil Akhir Pengujian Ke 3.....	47
Gambar 4.41 Hasil Akhir Pengujian Ke 4.....	47
Gambar 4.42 Hasil Akhir Pengujian Ke 5.....	48
Gambar 4.43 Hasil Akhir Pengujian Ke 6.....	48
Gambar 4.44 Hasil Akhir Pengujian Ke 7.....	49
Gambar 4.45 Hasil Akhir Pengujian Ke 8.....	49
Gambar 4.46 Hasil Akhir Pengujian Ke 9.....	50
Gambar 4.47 Hasil Akhir Pengujian Ke 10.....	50
Gambar 4.48 Hasil Akhir Pengujian Ke 11.....	51
Gambar 4.49 Hasil Akhir Pengujian Ke 12.....	51
Gambar 4.50 Hasil Akhir Pengujian Ke 13.....	52
Gambar 4.51 Hasil Akhir Pengujian Ke 14.....	52
Gambar 4.52 Hasil Akhir Pengujian Ke 15.....	53
Gambar 4.53 Hasil Akhir Pengujian Ke 16.....	53
Gambar 4.54 Hasil Akhir Pengujian Ke 17.....	54
Gambar 4.55 Hasil Akhir Pengujian Ke 18.....	54
Gambar 4.56 Hasil Akhir Pengujian Ke 19.....	55
Gambar 4.57 Hasil Akhir Pengujian Ke 20.....	55
Gambar 4.58 Hasil Akhir Pengujian Ke 21.....	56
Gambar 4.59 Hasil Akhir Pengujian Ke 22.....	56
Gambar 4.60 Hasil Akhir Pengujian Ke 23.....	57

Gambar 4.61 Hasil Akhir Pengujian Ke 24.....57
Gambar 4.62 Hasil Akhir Pengujian Ke 25.....58
Gambar 4.63 Hasil Akhir Pengujian Ke 26.....58



BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi khususnya jaringan computer saat ini menjadi hal yang paling mendasar. Akan sangat sulit jika didalam era teknologi informasi seperti sekarang ini tanpa menggunakan teknologi jaringan komputer. Hal ini dapat dilihat dari penggunaan jaringan baik secara umum maupun teknik. Dengan menggunakan jaringan *Wireless LAN* untuk mengakses jaringan pada era tertentu, maka harus dilakukan pengujian keamanan jaringan *Wireless LAN* agar tidak mengakibatkan terjadinya permasalahan dalam segi pengaksesan jaringan internet dalam pengiriman paket data.

Teknologi *Wireless* menawarkan berbagai macam kemudahan, kebebasan dan fleksibilitas yang tinggi. Teknologi *Wireless* menawarkan berbagai macam kemudahan, kebebasan dan fleksibilitas yang tinggi. Teknologi *Wireless* sangat nyaman untuk digunakan. Seorang user dapat mengakses internet kapan dan dimana saja asal masih berada dalam jangkauan sinyal *Wireless*. Masalah keamanan pada jaringan *Wireless* masih memerlukan perhatian yang serius, media transmisi data adalah udara yang bersifat broadcast. Sehingga diperlukan keamanan yang kuat untuk mendapatkan tingkat keamanan yang tinggi.

Access point adalah sebuah perangkat jaringan yang berisi sebuah transceiver dan antena untuk transmisi dan menerima sinyal ke dan dari *clients remote*. Dengan *access points* (AP) *clients wireless* bisa dengan cepat dan mudah

untuk terhubung kepada jaringan LAN kabel secara *wireless*. Agar kita lebih mudah untuk memahaminya maka bisa dibayangkan sebuah alat yang digunakan untuk menghubungkan alat-alat dalam suatu jaringan dari dan ke jaringan *wireless*. Secara garis besar, access point berfungsi sebagai pengatur lalu lintas data, sehingga memungkinkan banyak client dapat saling terhubung melalui jaringan (*Network*).

Dalam metode keamanan ini ada 2 jenis enkripsi yaitu, AES (*Advances Encryption Standard*) dan TKIP (*Temporal Key Integrity Protocol*). Diantara dua pendeskripsian ini, TKIP masih banyak kelemahan dibandingkan dengan AES menggunakan metode keamanan WPA2-PSK lebih aman dan tahan untuk ditembus dibanding tipe keamanan lainnya.

Sistem keamanan lainnya adalah WPA (*Wifi Protected Access*) yang menggunakan enkripsi TKIP (*Temporal Key Integrity Protocol*) yang memperbaiki kelemahan dari WEP dan menghasilkan keamanan yang lebih baik dari WEP. Kemudian diperbaharui kembali dengan keamanan yang lebih tinggi lagi menjadi WPA2 dengan menggunakan metode enkripsi AES yang merupakan enkripsi yang cukup kuat pada saat ini.

1.2 Identifikasi Masalah

1. Memberikan referensi kepada administrator jaringan untuk mengatasi serangan pada jaringan.
2. Memberikan referensi kepada administrator jaringan untuk mengetahui tingkat keamanan pada WEP, WPA-PSK dan WPA2-PSK

1.3 Rumusan Masalah

Pada saat ini keamanan dalam jaringan harus memerlukan perhatian cukup serius, karna hal ini merupakan salah satu factor penting dalam membangun sebuah jaringan, khususnya jaringan *wireless* yang melalui media udara . Keamanan lebih rentan dibanding dengan jaringan kabel. Rumusan masalah yang dibahas adalah :

1. Bagaimana mengetahui keamanan jaringan menggunakan *aircrack* pada keamanan WEP, WPA-PSK dan WPA2-PSK?
2. Bagaimana mengetahui kelebihan dan kelemahan teknik keamanan pada koneksi *wireless*?

1.4 Batasan Masalah

Untuk lebih terarah pada masalah analisa kejadian, Agar tidak terlalu melebar pembahasannya. Perlu ada batasan masalah yaitu perbandingan yang dilakukan hanya pada algoritma keamanan WEP, WPA-PSK dan WPA2-PSK.

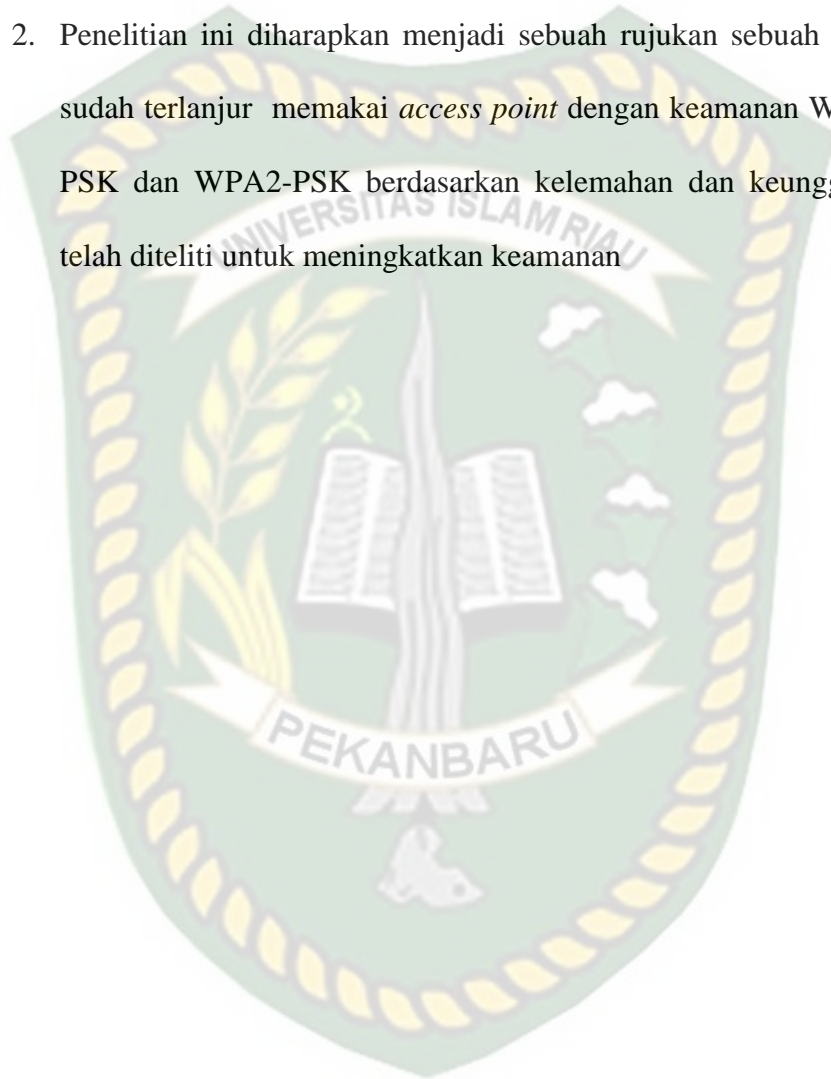
1.5 Tujuan

Tujuan yang ingin dicapai dari penulisan proposal skripsi ini adalah

1. Menganalisa jaringan wireless dengan menggunakan metode WEP, WPA dan WPA2-PSK
2. Membandingkan tingkat keamanan jaringan WEP, WPA dan WPA2-PSK

1.6 Manfaat

1. Memberikan informasi algoritma mana yg lebih layak dipakai dari WEP, WPA-PSK dan WPA2-PSK
2. Penelitian ini diharapkan menjadi sebuah rujukan sebuah instansi yg sudah terlanjur memakai *access point* dengan keamanan WEP, WPA-PSK dan WPA2-PSK berdasarkan kelemahan dan keunggulan yang telah diteliti untuk meningkatkan keamanan



Dokumen ini adalah Arsip Miik :

Perpustakaan Universitas Islam Riau

BAB II

LANDASAN TEORI

2.1 Studi Kepustakaan

Pada penelitian yang dilakukan oleh Desi Maya Sari, Muh. Yamin, dan LM. Baktiar Aksara (2017) yang berjudul “Analisis Sistem Keamanan Jaringan *Wireless* (WEP,WPAPSK/WPA2PSK) *Mac Address*, Menggunakan Metode *Penetration Testing*” menjelaskan bahwa walaupun memiliki keamanan jaringan, *wireless* masih dapat diserang oleh para *attacker* dengan menggunakan jenis serangan *cracking the encryption* dan *by passing WLAN authentication*. Oleh karena itu, diperlukan analisis terhadap sistem keamanan jaringan *wireless* untuk mensimulasikan bentuk-bentuk serangan terhadap keamanan jaringan. Berdasarkan hasil pengujian dan analisis diperoleh hasil bahwa sistem keamanan yang tepat untuk diterapkan pada jaringan *wireless* adalah sistem keamanan WPA-PSK/WPA2PSK.

Selanjutnya pada penelitian yang dilakukan oleh Bangkit Kurnia Ari Setyawan dan Melwin Syahrizal (2012) yang berjudul “Analisis Keamanan Jaringan *Wireless* yang Menggunakan *Captive Portal* (Studi Kasus: Warnet Fortran)” menjelaskan bahwa salah satu kelemahan teknologi pada saat ini adalah rentannya terhadap serangan para *attacker*. Hal itu dapat terjadi karena komunikasi yang berlangsung sangat terbuka. Maka diperlukan pengamanan yang berlapis agar dapat meminimalkan serangan tersebut. Dengan dilakukannya analisis terhadap keamanan jaringan *wireless* menggunakan metode *Man In The*

Middle Attack, para *attacker* tidak bisa mendapatkan informasi *username* dan *password* untuk mengakses jaringan wireless.

Selanjutnya penelitian yang dilakukan oleh Deris Setiawan dan Dian Palupi Rini (2009) yang berjudul “Analisis Perbandingan Sistem Keamanan WEP/WPA/RADIUS Pada Jaringan *Public Wireless Hotspot*” menjelaskan bahwa penggunaan *hotspot* saat ini telah menjadi standar pada perangkat-perangkat *mobile*. Namun masalah utama yang sering dihadapi saat penggunaan *hotspot* adalah keamanannya. Untuk mengetahui jenis keamanan yang tepat digunakan, maka dilakukan percobaan penetrasi *protocol* enkripsi WEP, WPA, dan RADIUS. Berdasarkan hasil percobaan, sistem keamanan RADIUS adalah metode otentikasi yang tangguh dan sulit untuk dipecahkan.

Selanjutnya pada penelitian yang dilakukan oleh Baihaqi, Yeni Yanti dan Zulfan (2018) yang berjudul “Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WI-FI” menjelaskan bahwa keamanan sistem jaringan *wireless* menjadi suatu keharusan untuk lebih diperhatikan, karena jaringan internet yang sifatnya publik dan global pada dasarnya tidak aman. Adanya lubang-lubang keamanan pada sistem jaringan menyebabkan kelemahan dan terbukanya lubang yang dapat digunakan *hacker*.

Selanjutnya penelitian yang dilakukan oleh Aji Supriyanto(2006) yang berjudul “Analisis Kelemahan Keamanan pada Jaringan Wireless” menjelaskan bahwa kelemahan jaringan wireless secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang

digunakan. Salah satu contoh penyebab kelemahan pada konfigurasi karena saat ini untuk membangun sebuah jaringan wireless cukup mudah.

Selanjutnya penelitian yang dilakukan oleh Siti Zaim (2015) yang berjudul “Apakah WPA/WPA2 Benar- Benar Aman? Deskripsi Paket Data Terenkripsi Pada WPA/WPA2” yang membedakan dengan WPA adalah WPA2 menggunakan *mixed mode* yang mendukung perangkat dengan WPA dan WPA2 pada *wireless network* yang sama. Terdapat perbedaan yang signifikan antara WPA dan WPA2 yaitu WPA2 menggunakan AES untuk enkripsi data, sedangkan WPA menggunakan TKIP.

2.2 Dasar Teori

2.2.1 WEP(*Wired Equivalent Privacy*)

Shared Key atau WEP (*Wired Equivalent Privacy*) adalah suatu metode pengamanan jaringan nirkabel, disebut juga dengan *Shared Key Authentication* adalah metode otentikasi yang membutuhkan penggunaan WEP. Enkripsi WEP menggunakan kunci yang dimasukan (oleh administrator) ke client maupun *access point*. Kunci ini harus cocok dengan yang diberikan akses point ke client, dengan yang dimasukan client untuk autentikasi menuju *access point*.

Pada standart 802.11 merupakan enkripsi opsional dan standart otentikasi yang diterapkan pada beberapa *wireless network interface card* (NIC) dan didukung beberapa vendor *access point*. Sesudah pengguna dikonfigurasi pada *access point* dan pengguna, semua komunikasi yang dikirim melalui udara, dienkripsi sehingga menyediakan koneksi yang aman dan sulit untuk disusupi. (Deris dan Dian,2009)

2.2.2 WPA-PSK (*Wi-Fi Protected Access – Pre Shared Key*)

WPA-PSK (*Wi-Fi Protected Access – Pre Shared Key*) adalah pengamanan jaringan nirkabel dengan menggunakan metode WPA-PSK jika tidak ada autentikasi server yang digunakan. Dengan demikian *access point* dapat dijalankan dengan mode WPA tanpa menggunakan bantuan komputer lain sebagai server. Cara mengkonfigurasinya juga cukup sederhana. Perlu diketahui bahwa tidak semua *access point* akan mempunyai fasilitas yang sama dan tidak semua *access point* menggunakan cara yang sama dalam mendapatkan *Shared-Key* yang akan dibagikan ke client.

Dan WPA menawarkan enkripsi kunci yang dinamis dan otentikasi secara manual. Beberapa vendor telah mendukung WPA, sehingga mempermudah implementasinya. WPA menyediakan pengaturan dan implementasi yang cukup mudah tanpa melakukan perubahan yang berarti pada desain hardware WLAN 802.11. Fitur-fitur keamanan yang lebih kuat sangat berhubungan dengan kekuatan pada metode enkripsinya. (Deris dan Dian,2009)

2.2.3 WPA2 - PSK

WPA2 adalah sertifikasi produk yang tersedia melalui Wi-Fi Alliance. WPA2 Sertifikasi hanya menyatakan bahwa peralatan nirkabel yang kompatibel dengan standar IEEE 802.11i. WPA2 sertifikasi produk yang secara resmi menggantikan wired equivalent privacy (WEP) dan fitur keamanan lain yang asli standar IEEE 802.11. WPA2 tujuan dari sertifikasi adalah untuk mendukung wajib tambahan fitur keamanan standar IEEE 802.11i yang tidak sudah termasuk untuk produk-produk yang mendukung WPA. Update WPA2/WPS IE yang

mendukung WPA2 fitur berupa WPA2 Enterprise IEEE 802.1X menggunakan otentikasi dan WPA2 Personal menggunakan tombol preshared (PSK).

2.2.4 Perbedaan WEP, WPA-PSK dan WPA2-PSK

2.2.4.1 WEP

1. Masalah kunci yang lemah dengan menggunakan algoritma RC4 dapat dengan mudah dipecahkan
2. WEP menggunakan kunci yang bersifat statis
3. Masalah integritas pesan Cyclic Redundancy Check (CRC-32)
4. Masalah initialization vector (IV) WEP

Serangan-serangan pada kelemahan WEP antara lain :

1. Serangan terhadap kelemahan inisialisasi vektor (IV), sering disebut FMS attack. FMS singkatan dari nama ketiga penemu kelemahan IV yakni Fluhrer, Mantin, dan Shamir. Serangan ini dilakukan dengan cara mengumpulkan IV yang lemah sebanyak-banyaknya. Semakin banyak IV lemah yang diperoleh, semakin cepat ditemukan kunci yang digunakan
2. Mendapatkan IV yang unik melalui packet data yang diperoleh untuk diolah untuk proses cracking kunci WEP dengan lebih cepat. Cara ini disebut chopping attack, pertama kali ditemukan oleh hikari. Teknik ini hanya membutuhkan IV yang unik sehingga mengurangi kebutuhan IV yang lemah dalam melakukan cracking WEP.
3. Kedua serangan diatas membutuhkan waktu dan packet yang cukup, untuk mempersingkat waktu, para hacker biasanya melakukan traffic injection. Traffic Injection yang sering dilakukan adalah dengan cara mengumpulkan

packet ARP kemudian mengirimkan kembali ke access point. Hal ini mengakibatkan pengumpulan initial vektor lebih mudah dan cepat. Berbeda dengan serangan pertama dan kedua, untuk serangan traffic injection, diperlukan spesifikasi alat dan aplikasi tertentu yang mulai jarang ditemui di toko-toko, mulai dari chipset, versi firmware, dan versi driver serta tidak jarang harus melakukan patching terhadap driver dan aplikasinya.

Kelebihan WEP

Saat user hendak mengkoneksikan laptopnya, user tidak melakukan perubahan setting apapun, semua serba otomatis, dan saat pertama kali hendak browsing, user akan diminta untuk memasukkan *username* dan *password*, hampir semua komponen *wireless* sudah mendukung protokol ini.

2.2.4.2 WPA

Meningkatkan enkripsi data dengan teknik *Temporal Key Integrity Protocol* (TKIP). enkripsi yang digunakan masih sama dengan WEP yaitu RC4, karena pada dasarnya WPA ini merupakan perbaikan dari WEP dan bukan suatu level keamanan yang benar – benar baru, walaupun beberapa device ada yang sudah mendukung enkripsi AES yaitu enkripsi dengan keamanan yang paling tinggi.

Kelemahan WPA:

Kelemahan WPA sampai saat ini adalah proses kalkulasi enkripsi/dekripsi yang lebih lama dan data overhead yang lebih besar. Dengan kata lain, proses transmisi data akan menjadi lebih lambat dibandingkan bila anda menggunakan protokol WEP. Belum semua *wireless* mendukung.

2.2.4.3 WPA2-PSK

WPA2/PSK adalah security terbaru untuk wireless, dan lebih bagus dari WEP dan WPA-PSK, tetapi masih bisa untuk dicrack atau disadap tetapi sangat memakan banyak waktu. Dalam WPA2-PSK ada dua jenis decryption, Advanced Encryption Standard (AES) dan Temporal Key Integrity Protocol (TKIP). TKIP banyak kelemahan oleh itu lebih baik anda gunakan AES. Panjang key adalah 8-63, anda boleh memasukkan sama ada 64 hexadecimal atau ASCII(seperti biasa). Oleh karena itu saya sarankan kepada anda , pakai WPA2-PSK(AES), lebih secure dan lama untuk crack. Tapi ingat! Anda perlu pastikan wireless router anda dan wifi adapter anda support WPA dan WPA2.

Dalam WPA2 / WPS IE terbagi menjadi 2 update keamanan :

A. WPA 2 Enterprise IEEE 802.1X

Sebelum masuk ke WPA2 enterprise, berikut ini sedikit penjelasan mengenai WPA2. WPA2 merupakan sertifikasi prodek yang tersedia melalui wi-fi alliance. Untuk WPA2 enterprise ini memiliki 3 bagian utama yang terlibat, diantaranya adalah supplicant (client), authenticator dan authentication server. WPA2 enterprise menggunakan 802.1 x sebagai passwordnya dengan protocol EAP (contohnya EAP-TLS dan EAP-TTLS).

B. WPA2 Personal

WPA2 personal menggunakan Pre-Shared Key sebagai passwordnya, namun bisa di sadap dengan metode dictionary attack/brute force attack. Karena

itu WPA2 personal ini tidak cocok digunakan untuk sistem pengamanan perusahaan besar.

Kelebihan WPA2-PSK

1. Access point dapat dijalankan dengan mode WPA tanpa menggunakan bantuan komputer lain sebagai server
2. Cara mengkonfigurasikannya juga cukup sederhana

Kelemahan WPA2-PSK

Satu satunya kelemahan WPA2-PSK adalah ketika sebuah client melakukan koneksi ke AP dimana terjadinya proses handshake, kita bisa melakukan Bruto Force yang akan mencoba satu persatu password yang ada dengan didapatkan dari proses handshake. Melakukan Bruto Force adalah melakukan dengan menggunakan dictionary file yang artinya kita harus mempunyai file berisi passpharase yang akan di coba satu persatu dengan paket handshake untuk mencari keys yg digunakan tersebut (Siti Zaim 2015).

2.2.5 Access Point

Access point adalah alat bantu pada jaringan *wireless* atau WLAN *access point* menerima dan memancarkan kembali data yang berupa gelombang. *Access point* memnghubungkan antara komputer satu dengan yang lain pada WLAN dan kadang berfungsi pula menjadi jembatan (Bridge) antara WLAN dengan jaringan yang menggunakan kabel. *Access point* memiliki fungsi yang sama seperti *hub* bagi jaringan menggunakan kabel. WLAN berukuran kecil cukup menggunakan satu *access point* saja namun WLAN yang besar membutuhkan beberapa *access point* sekaligus. (Edi s. Mulyanto, 2008)

2.2.6 Aircrack

Aircrack-ng adalah berbagai kumpulan aplikasi yang berguna untuk menilai dan mengukur tingkat keamanan pada jaringan WiFi. Aircrack bekerja pada jaringan WiFi yang mendukung monitoring mode dan bisa mendeteksi trafik jaringan dari 802.11a, 802.11b and 802.11g.

2.2.6.1 Fungsi Aircrack-ng






Aircrack-ng berfokus pada keamanan WIFI yang berbeda :



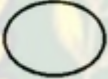
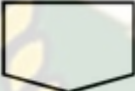
1. Pemantauan: Packet capture dan ekspor data ke file teks untuk diproses lebih lanjut oleh aplikasi pihak ketiga.
2. Menyerang: Serangan ulang, deauthentication, membuat akses point palsu dan melalui via injeksi paket.
3. Pengujian: Memeriksa kartu WiFi dan kemampuan driver (capture and injection).
4. Cracking: Cracking pada WEP dan WPA PSK (WPA 1 dan 2).

Semua alat adalah command line yang memungkinkan untuk scripting berat. Banyak GUI yang memanfaatkan fitur ini. Aircrack-ng bekerja terutama pada Linux tapi juga Windows, OS X, FreeBSD, OpenBSD, NetBSD, serta Solaris dan bahkan eComStation 2.

2.2.7 Flowchart

Flowchart adalah bagan-bagan yang mempunyai arus yang menggambarkan langkah-langkah penyelesaian suatu masalah. *Flowchart* merupakan cara penyajian dari suatu algoritma. Simbol *flowchart* dan fungsinya dapat dilihat pada tabel sebagai berikut :

No	Simbol	Nama	Fungsi
1		Terminator	Permulaan / pengakhiran program
2		Flow Line	Arah aliran program
3		Preparation	Proses inialisasi/pemberian nilai awal
4		Process	Proses pengolahan data
5		Input/Ouput Data	Proses input/output data,parameter, informasi

6		Predefined Process	Permulaan sub program / proses menjalankan sub program
7		Decision	Perbandingan pernyataan, penyeleksian data yang memberikan pilihan untuk langkah selanjutnya
8		On Page Connector	Penghubung bagian-bagian flowchart yang berada pada satu halaman
9		Off page Connector	Penghubung bagian-bagian flowchart yang berada pada halaman berbeda

Tabel 2.1 Simbol dan Fungsi *Flowchart*

BAB III

METODOLOGI PENELITIAN

3.1 Alat Dan Bahan Penelitian

Alat

Disini penulis menggunakan alat untuk menganalisa apa yang dirancang oleh penulis. Agar dengan menggunakan alat tersebut penulis dapat menghasilkan analisa yang lebih baik.

Bahan Penelitian

Disini penulis menggunakan bahan penelitian dengan riset setiap jurnal-jurnal, tesis, skripsi dan panduan lainnya agar dapat memahami isi penelitian yang dirancang oleh penulis, maka dari itu penulis sangat membutuhkan alat-alat yang diperlukan seadannya untuk penulis, agar sesuatu yang dirancang penulis sesuai rencana yang direncanakannya.

Maka dari itu, Disini penulis menggunakan alat-alat tersebut yaitu ada perangkat keras (*Hardware*) dan juga perangkat lunak (*Software*) yang penulis gunakan, Agar dapat menghasilkan yang lebih baik maka dari itu penulis membutuhkan alat tersebut sesuai dengan kebutuhan penulis.

3.1.1 Spesifikasi Perangkat Keras (Hardware)

Spesifikasi perangkat keras (*Hardware*) adalah bahan digunakan oleh penulis, Sebagai alat yang digunakan untuk melengkapi suatu rancangan yang dirancang penulis sebagai berikut:

No	Perangkat Keras	Spesifikasi	Fungsi
1	Laptop	<ul style="list-style-type: none"> • Processor Intel Coleron • Ram 2.00 GB • Harddisk 320 GB 	<ul style="list-style-type: none"> • Sebagai media yang digunakan penulis
2	Acces Point	<ul style="list-style-type: none"> • IEEE Standards: IEEE 802.3, 802.3u • IEEE Standards: IEEE 802.3, 802.3u 	<ul style="list-style-type: none"> • Untuk menilai keamanan jaringan

Tabel 3.1 Perangkat Keras

3.1.2 Spesifikasi Perangkat Lunak (Software)

Perangkat lunak (*Software*) ini adalah sebagai alat media untuk melengkapi pengujian yang direncanakan oleh penulis tersebut, maka dari itu penulis menampilkan perangkat lunak sebagai berikut:

No	Perangkat Lunak	Spesifikasi	Fungsi
1	Kali Linux	7	Disini penulis menggunakan kali linux untuk suatu analisa yang dibuat.
2	Aircrack	1.5.7	Menilai dan Mengukur tingkat keamanan jaringan <i>Wi-Fi</i> .

Tabel 3.2 Perangkat Lunak

3.2 Metode Penelitian

Metode adalah kerangka kerja untuk melakukan suatu tindakan, atau suatu kerangka berpikir untuk menyusun suatu gagasan yang terarah dan terkait dengan maksud dan tujuan. Metode ilmiah atau proses ilmiah merupakan proses keilmuan untuk memperoleh pengetahuan secara sistematis berdasarkan bukti fisik.

Metode penelitian yang tepat dan benar semakin dirasakan urgensinya bagi keberhasilan suatu penelitian. Satu hal yang penting dalam setiap penelitian adalah perumusan metodologi penelitian. Melalui metodologi harus dengan jelas tergambar bagaimana penelitian tersebut dilaksanakan yang disusun dan tertata secara sistematis. Selain melalui metodologi juga dapat dilihat bagaimana landasan teori tentang rancangan penelitian (*research design*), model yang digunakan (didahului dengan rancangan percobaan/penelitian eksperimen) maupun teknik-teknik yang lumrah digunakan dalam pengumpulan pengolahan dan analisa data. Metode yang digunakan antara lain metode sejarah, metode deskriptif, metode survei (menyelidiki gejala, fakta secara faktual), metode percobaan (eksperimen), metode studi kasus (suatu objek spesifik), metode

koperatif yang menjawab keadaan sebab akibat dengan menganalisis faktor penyebab utama serta studi kepustakaan.

Sedangkan penelitian merupakan suatu proses mencari sesuatu secara sistematis dalam waktu yang relatif lama dengan menggunakan metode ilmiah dengan prosedur maupun aturan yang berlaku. Penelitian itu sendiri terjadi karena adanya dorongan rasa ingin tahu mengenai sesuatu hal yang sedang terjadi dilingkungan sekitar. Seseorang melakukan penelitian untuk mencari jawaban dari permasalahan yang sedang terjadi. Penelitian terdiri atas beberapa tahapan yang saling terkait antara satu dengan yang lainnya. Dimana tahapan-tahapan itu pada umumnya terdiri dari:

1. Identifikasi masalah
2. Perumusan masalah
3. Penelusuran pustaka
4. Rancangan penelitian
5. Pengumpulan data
6. Pengolahan data Penyimpulan hasil

Kegiatan untuk mengembangkan ilmu pengetahuan dan teknologi dapat dilakukan dengan penelitian. Penelitian itu sendiri bertujuan untuk menciptakan ilmu pengetahuan baru atau menerapkan teknologi untuk memecahkan suatu masalah. Penelitian dilakukan dengan metode ilmiah. Jadi, penelitian adalah kegiatan yang menggunakan metode ilmiah untuk mengungkapkan ilmu pengetahuan atau menerapkan teknologi. Perkembangan suatu bidang ilmu

pengetahuan dipengaruhi oleh banyak faktor, mulai dari kepentingan atau kebutuhan lahirnya teori baru, keberadaan teori lama sebagai batu pijakan, pengaruh teori dari bidang ilmu pengetahuan lainnya, serta metodologi ilmu pengetahuan yang dipergunakan.

Riset atau penelitian sering dideskripsikan sebagai suatu proses investigasi untuk menemukan dan menginterpretasikan fakta yang ditemukan. Sebuah riset yang baik akan menghasilkan:

1. Produk atau inovasi baru yang dapat langsung dipakai oleh industri (bukan hanya sebatas prototipe)
2. Publikasi di jurnal internasional

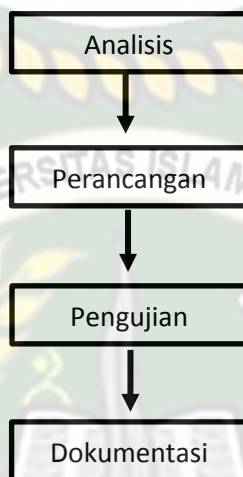
Dalam melakukan penelitian terdapat langkah-langkah sistematis yang harus dilakukan. Hal ini berupa penerapan metode ilmiah dalam penelitian yang bertujuan agar keluaran penelitian dapat dipertanggung jawabkan kebenarannya. Penelitian yang dilakukan dalam bidang sistem informasi merupakan suatu proses pengumpulan dan menganalisa data yang ada secara sistematis untuk memperoleh jawaban atau penjelasan suatu fenomena yang diamati.

3.3 Jenis Data

1. Data sekunder yaitu suatu data yang diperoleh melalui daftar pustaka, buku dan literatur- literatur yang berhubungan dengan masalah yang sedang penulis buat dan diambil dalam bentuk yang sudah jadi atau publikasi. Studi literatur adalah melakukan data dengan membaca buku-buku yang berhubungan dengan permasalahan yang dibahas.

2. Data primer yaitu data-data yang diperoleh penulis secara langsung di LAB IT.

3.4 Metode Pengumpulan Data



Gambar 3.1 Skema Prosedur Penelitian

Proses pengumpulan data adalah untuk mendapatkan data yang benar dan menyakinkan, agar hasil yang dicapai tidak menyimpang dari tujuan yang telah ditetapkan sebelumnya, penulis melakukan langkah-langkah penelitian sebagai berikut

1. Analisa

Metode awal dalam melakukan penelitian yaitu analisa, analisa digunakan untuk menganalisa sebuah rancangan yang dibangun pada pembuatan suatu desain yang telah dibuat penulis, hingga pengujian jaringan tersebut apakah hasil yang didapat dari rancangan yang diimplementasikan akan mendapatkan hasil yang baik.

2. Perancangan

Metode kedua tahap ini akan menterjemahkan spesifikasi kebutuhan yang telah didapat pada tahap analisis ke dalam bentuk arsitektural perangkat lunak untuk diimplementasikan kepada yang dibuat.

3. Pengujian

Metode ketiga dalam tahap pengujian dilakukan dengan menggunakan aplikasi Aircrack dan Commview untuk mendapatkan hasil simulasi yang dibuat dimana hasil dari pengujian

4. Dokumentasi

Metode keempat pada proses dokumentasi, penulis juga melakukan studi pustaka, membaca dan mempelajari dokumen- dokumen, buku- buku acuan dan dokumentasi video, serta sumber lainnya yang berkaitan dengan penelitian untuk dijadikan referensi

3.5 Pengembang dan Perancangan Sistem

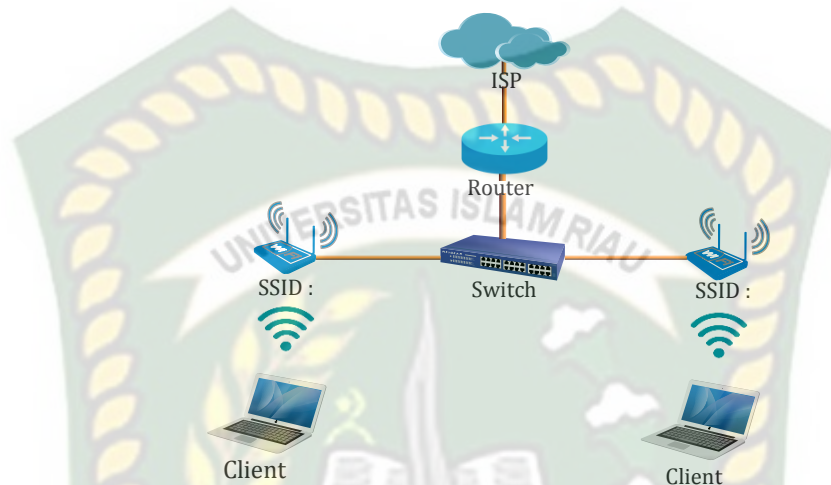
3.5.1 Desain Topologi

Pada simulasi ini menggunakan jaringan local yang terdiri 2 PC *notebook*, 2 *access point* yang terhubung dari *switch* dan *router* yang menghubungkan ke *switch*, lalu *router* terhubung dari *ISP* yang memberikan jaringan internet.

3.5.1.1 Topologi Physical LAB IT

Berdasarkan gambar 3.2 adalah contoh topologi labor teknik informatika yang berjalan saat ini, *gateway* dari topologi ini adalah dari *ISP* yaitu *Indihome*,

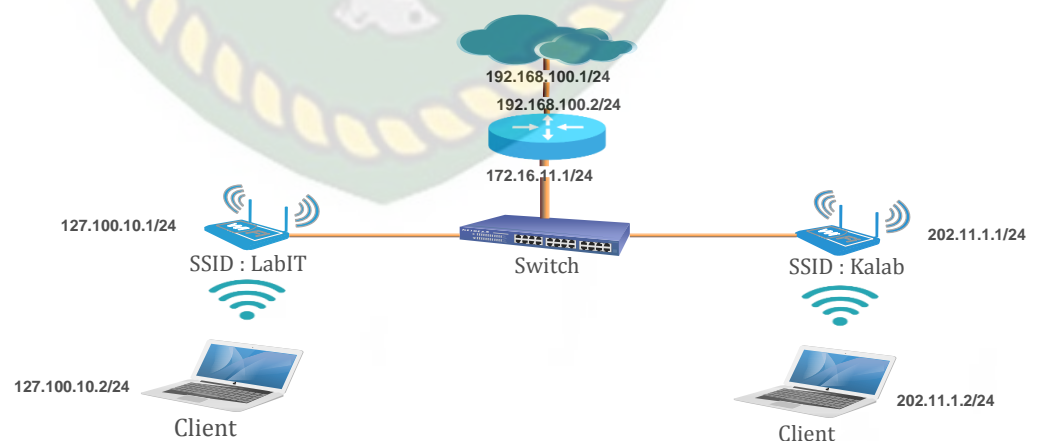
kemudian jaringan tersebut disebar menjadi beberapa jaringan. Jaringan tersebut disebar menggunakan dua buah *access point* dengan SSID Kalab, dan LabIT



Gambar 3.2 Rancangan Topologi Pysical Lab IT

3.5.1.2 Topologi Logical LAB IT

Berdasarkan gambar 3.3 hampir sama dengan topologi physical hanya saja topologi logical menggambarkan secara logika bagaimana hubungan yang terjadi antar masing-masing komputer dalam jaringan yang tidak dapat kita lihat



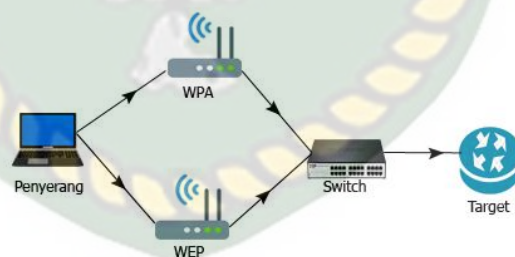
Gambar 3.3 Rancangan Topologi Logical Lab IT

3.6 Simulasi Serangan Terhadap WEP, WPA-PSK dan WPA2-PSK

3.6.1 Rancangan Serangan

Dari gambar 3.4 menggambarkan tahapan dalam melakukan pengujian. Pada tahapan ini dapat dilihat bahwa penyerang akan meretas dua buah *access point* yang mana masing-masing *access point* memiliki sandi yang berbeda enkripsi yaitu WPA dan WEP. Penyerang akan melakukan monitoring jaringan terlebih dahulu menggunakan aplikasi monitoring jaringan yaitu *CommView*. Setelah SSID target telah didapatkan, pengujian selanjutnya adalah melakukan pengujian untuk mendapatkan kata sandi *wifi* dari kedua *access point* tersebut. Hasil akhir pengujian ini adalah masuk ke *access point* untuk mengakses *router*.

Dari pengujian tersebut data akan dioleh dan menghasilkan sebuah kesimpulan enkripsi mana yang memiliki tingkat keamanan yang lebih baik.



Gambar 3.4 Simulasi Serangan Terhadap WEP, WPA-PSK dan WPA2-PSK

Serangan-serangan pada WEP

Adapun beberapa serangan terhadap enkripsi WEP antar lain :

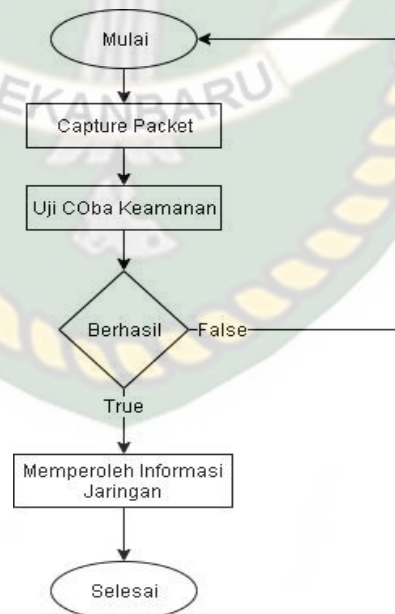
1. Serangan terhadap kelemahan inisialisasi vektor (IV), sering disebut FMS attack. FMS singkatan dari nama ketiga penemu kelemahan IV yakni Fluhrer, Mantin, dan Shamir. Serangan ini dilakukan dengan cara mengumpulkan IV yang lemah sebanyak-banyaknya. Semakin banyak IV lemah yang diperoleh, semakin cepat ditemukan kunci yang digunakan
2. Mendapatkan IV yang unik melalui packet data yang diperoleh untuk diolah untuk proses cracking kunci WEP dengan lebih cepat. Cara ini disebut chopping attack, pertama kali ditemukan oleh hikari. Teknik ini hanya membutuhkan IV yang unik sehingga mengurangi kebutuhan IV yang lemah dalam melakukan cracking WEP.
3. Kedua serangan diatas membutuhkan waktu dan packet yang cukup, untuk mempersingkat waktu, para hacker biasanya melakukan traffic injection. Traffic Injection yang sering dilakukan adalah dengan cara mengumpulkan packet ARP kemudian mengirimkan kembali ke access point. Hal ini mengakibatkan pengumpulan initial vektor lebih mudah dan cepat. Berbeda dengan serangan pertama dan kedua, untuk serangan traffic injection, diperlukan spesifikasi alat dan aplikasi tertentu yang mulai jarang ditemui di toko-toko, mulai dari chipset, versi firmware, dan versi driver serta tidak jarang harus melakukan patching terhadap driver dan aplikasinya.

3.6.2 Serangan terhadap WPA-PSK dan WPA2-PSK

Adapun beberapa serangan terhadap enkripsi WEP antar lain :

1. Tidak ada konfigurasi atau *Poor Security*
2. Tidak ada pengaturan batas
3. Lokasi yang tidak aman
4. Pengguna tidak mengatur jaringan dengan baik
5. Adanya *Rogue Acces Point*
6. Kelemahan dalam memantau jaringan
7. *MAC fitering*
8. Standart enkripsi yang tidak memadai

3.7 Flochart serangan WEP, WPA-PSK dan WPA2-PSK



Gambar 3.5 Flochart Serangan WEP, WPA-PSK dan WPA2-PSK

Berdasarkan gambar 3.5 diatas dapat dilihat bahwa flowchart tersebut menggambarkan alur proses dalam melakukan serangan pada enkripsi WEP, WPA-PSK dan WPA2-PSK

3.8 Rancangan proses pengujian keamanan jaringan

Pada gambar 3.6 penulis akan melakukan rancangan tersebut, pada gambar 3.6 ini menampilkan monitoring untuk jaringan terdeteksi pada area penulis.

```
CH 12 ][ Elapsed: 36 s ][ 2019-12-17 15:44 ][ interface wlan0 down
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
10:FE:ED:2F:F2:52	-53	78	10	0	1	54	WPA2	TKIP	PSK	TP-LINK_2FF252
B0:4E:26:B9:26:EA	-52	71	2356	147	11	270	OPN		PSK	ADAM_KOS_B
9C:71:3A:86:C2:84	-68	98	0	0	7	130	WPA2	CCMP	PSK	Zero
B0:4E:26:A1:83:46	-74	75	0	0	1	270	OPN		PSK	ADAM_KOS_A
78:58:60:80:2C:18	-81	6	0	0	8	130	WPA2	CCMP	PSK	RUSLI TELUK PAMAN
A0:F8:49:ED:44:62	-84	5	0	0	11	130	WPA2	CCMP	MGT	seamless@wifi.id
A0:F8:49:ED:44:61	-88	8	7	0	11	130	OPN		PSK	@wifi.id
0C:80:63:09:0B:22	-86	20	0	0	11	270	OPN		PSK	ADAM_KOS_C
78:58:60:80:22:0C	-88	3	0	0	3	130	WPA2	CCMP	PSK	ENDANG WONGSO
7A:58:60:80:22:0D	-88	2	0	0	3	130	WPA2	CCMP	PSK	<length: 6>

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	DA:A1:19:EC:0A:2F	-49	0 - 1	0	7	
(not associated)	DA:A1:19:12:F3:1B	-61	0 - 1	0	16	
(not associated)	1E:33:75:6A:BF:64	-70	0 - 1	0	5	
(not associated)	E8:AC:AD:91:5C:20	-74	0 - 1	0	7	
10:FE:ED:2F:F2:52	A8:1B:5A:D2:76:BC	-42	0 - 6	62	17	

Gambar 3.6 Monitoring Jaringan yang Terdeteksi

Pada gambar 3.7 adalah hasil dari rancangan penulis yang telah didapatkan dengan waktu 8 detik dengan metode WPA2-PSK enkripsi TKIP dengan password Uirunggul2020 yang telah ditemukan.

```
Aircrack-ng 1.5.2
[00:00:08] 5671/488132 keys tested (573.50 k/s)
Time left: 14 minutes, 1 second 1.16%
KEY FOUND! [ Uirunggul2020 ]

Master Key   : 2D E0 F1 37 8B 54 DB 59 98 CF A8 87 B3 63 0F 49
              BB 18 92 AE 2B 67 84 EE 5F 89 74 95 26 52 35 BC
Transient Key : AC 69 12 55 DD DC A6 11 0A B5 EB FF 3A 7C AF 6F
              96 47 8A 9D 94 71 99 C6 57 2D CF 0A E4 6D C5 0A
              DC 16 66 13 75 FB 46 31 3D 8A 56 15 5E F8 A6 F7
              13 6C 5E C0 E1 CF 33 E8 9A 76 E3 D2 46 C2 81 C7
EAPOL HMAC   : 0A 78 C1 24 A5 C9 FA 45 C4 8D C6 B1 CD AD 8C 01
root@Skripsi:~#
```

Gambar 3.7 Hasil Akhir Pengujian

BAB IV

HASIL DAN PEMBAHASAN

4.1 Melakukan Konfigurasi Pada Acces Point

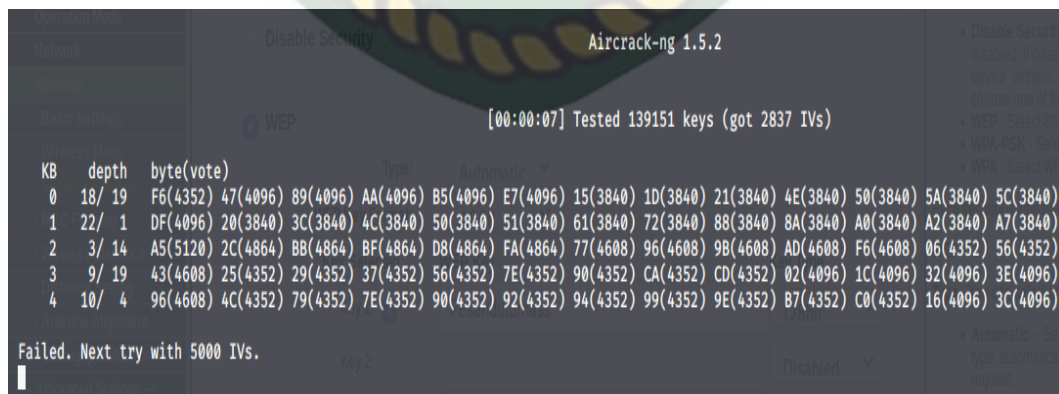
Dalam pengujian kepada *Acces Point* tersebut penulis akan melakukan pengujian kepada metode masing-masing. Hal ini akan membutuhkan waktu pengujian kepada metode WEP sebanyak 15 pengujian, WPA-PSK sebanyak 20 pengujian dan WPA2-PSK sebanyak 25 pengujian.

Dalam pengujian ini penulis akan melampirkan hasil akhir WEP, WPA-PSK dan WPA2-PSK pada Bab berikut ini.

4.2 Hasil Akhir Pengujian Metode WEP

Pengujian terhadap metode WEP tersebut akan dilakukan pengujian sebanyak 15 kali pengujian gagal dan 1 pengujian akhir yang benar total pengujian pada WEP sebanyak 16 pengujian.

Pada gambar 4.1 adalah hasil akhir pengujian pada metode WEP



```
Aircrack-ng 1.5.2
[00:00:07] Tested 139151 keys (got 2837 IVs)

KB  depth  byte(vote)
0   18/ 19   F6(4352) 47(4096) 89(4096) AA(4096) B5(4096) E7(4096) 15(3840) 1D(3840) 21(3840) 4E(3840) 50(3840) 5A(3840) 5C(3840)
1   22/  1   DF(4096) 20(3840) 3C(3840) 4C(3840) 50(3840) 51(3840) 61(3840) 72(3840) 88(3840) 8A(3840) A0(3840) A2(3840) A7(3840)
2    3/ 14   A5(5120) 2C(4864) BB(4864) BF(4864) D8(4864) FA(4864) 77(4608) 96(4608) 9B(4608) AD(4608) F6(4608) 06(4352) 56(4352)
3    9/ 19   43(4608) 25(4352) 29(4352) 37(4352) 56(4352) 7E(4352) 90(4352) CA(4352) CD(4352) 02(4096) 1C(4096) 32(4096) 3E(4096)
4   10/  4   96(4608) 4C(4352) 79(4352) 7E(4352) 90(4352) 92(4352) 94(4352) 99(4352) 9E(4352) B7(4352) C0(4352) 16(4096) 3C(4096)

Failed. Next try with 5000 IVs.
```

Gambar 4.1 Hasil Akhir Pengujian ke 1

Pada gambar 4.2 adalah hasil akhir pengujian pada metode WEP

```

Aircrack-ng 1.5.2

[00:00:05] Tested 136417 keys (got 10915 IVs)

KB  depth  byte(vote)
0   3/ 4    C3(15104) 13(14592) 00(14336) 37(14336) 44(14336) 7A(14336) E8(14336) BF(14080) DE(14080) 06(13824) 6F(13824) C9(13824) D6(13824)
1   28/ 1    D0(13056) 00(12800) 0B(12800) 23(12800) 2D(12800) 58(12800) A5(12800) 03(12544) 1C(12544) 1F(12544) 38(12544) 4A(12544) 4B(12544)
2   27/ 2    DC(13056) 17(12800) 2C(12800) 32(12800) 5D(12800) 8E(12800) AD(12800) DD(12800) EA(12800) 0E(12544) 1F(12544) 6D(12544) 9A(12544)
3   7/ 44    87(13824) 0C(13568) 26(13568) 30(13568) 52(13568) 61(13568) 71(13568) 82(13568) 9B(13568) B6(13568) 39(13312) 40(13312) 53(13312)
4   18/ 58   FC(13568) 20(13312) 7B(13312) B6(13312) 02(13056) 51(13056) 60(13056) 83(13056) 9D(13056) A5(13056) D2(13056) EB(13056) 44(12800)

Failed. Next try with 15000 IVs.

```

Gambar 4.2 Hasil Akhir Pengujian ke 2

Pada gambar 4.3 adalah hasil akhir pengujian pada metode WEP

```

Aircrack-ng 1.5.2

[00:00:10] Tested 126085 keys (got 22 IVs)

KB  depth  byte(vote)
0   20/ 21   FD( 256) 00(  0) 01(  0) 02(  0) 03(  0) 04(  0) 05(  0) 07(  0) 08(  0) 09(  0) 0A(  0) 0B(  0) 0C(  0)
1   18/ 19   F4( 256) 00(  0) 01(  0) 02(  0) 03(  0) 04(  0) 05(  0) 06(  0) 07(  0) 09(  0) 0A(  0) 0B(  0) 0C(  0)
2   21/  2   F4( 256) 00(  0) 01(  0) 02(  0) 04(  0) 05(  0) 06(  0) 07(  0) 08(  0) 09(  0) 0A(  0) 0B(  0) 0C(  0)
3   0/  7    1C( 512) 11( 256) 12( 256) 22( 256) 2C( 256) 40( 256) 57( 256) 58( 256) 67( 256) 85( 256) 86( 256) 9B( 256) A8( 256)
4   0/  4    61( 512) 13( 256) 15( 256) 18( 256) 25( 256) 36( 256) 38( 256) 41( 256) 4F( 256) 73( 256) 78( 256) 81( 256) 84( 256)

Failed. Next try with 5000 IVs.

```

Gambar 4.3 Hasil Akhir Pengujian ke 3

Pada gambar 4.4 adalah hasil akhir pengujian pada metode WEP

```

Aircrack-ng 1.5.2
[00:00:05] Tested 173831 keys (got 22 IVs)

KB  depth  byte(vote)
0  21/186  FF( 256) 00(  0) 02(  0) 03(  0) 04(  0) 05(  0) 06(  0) 07(  0) 08(  0) 09(  0) 0A(  0) 0B(  0) 0C(  0)
1  2/  3   06( 512) 00( 256) 0B( 256) 15( 256) 16( 256) 1D( 256) 20( 256) 29( 256) 48( 256) 4D( 256) 5A( 256) 77( 256) 8A( 256)
2  2/  3   CD( 512) 0D( 256) 1B( 256) 3C( 256) 64( 256) 74( 256) 77( 256) 83( 256) 8C( 256) 9D( 256) A1( 256) BA( 256) BB( 256)
3  1/  3   DF( 512) 0D( 256) 12( 256) 17( 256) 44( 256) 57( 256) 74( 256) 77( 256) 9A( 256) 9B( 256) C7( 256) D2( 256) D7( 256)
4  1/  4   C5( 512) 00( 256) 0B( 256) 28( 256) 2B( 256) 2C( 256) 48( 256) 4B( 256) A9( 256) AD( 256) BB( 256) BC( 256) C2( 256)

Failed. Next try with 5000 IVs.

```

Gambar 4.4 Hasil Akhir Pengujian ke 4

Pada gambar 4.5 adalah hasil akhir pengujian pada metode WEP

```

Aircrack-ng 1.5.2
[00:00:09] Tested 159877 keys (got 2958 IVs)

KB  depth  byte(vote)
0  25/ 35  CD(4352) 3B(4096) 5A(4096) 6D(4096) 84(4096) 8C(4096) 92(4096) A2(4096) A5(4096) B2(4096) CC(4096) F6(4096) 0D(3840)
1  18/  1  C2(4352) 2B(4096) 31(4096) 46(4096) 4B(4096) 4C(4096) 5C(4096) 6A(4096) 70(4096) 7E(4096) 90(4096) 94(4096) C8(4096)
2  5/ 15  E0(5120) 3E(4864) 64(4864) 9A(4864) F1(4864) F4(4864) 67(4608) B5(4608) C5(4608) CC(4608) 03(4352) 52(4352) 17(4096)
3  25/  3  E5(4352) 0C(4096) 10(4096) 28(4096) 4B(4096) 59(4096) 87(4096) 99(4096) 9E(4096) C1(4096) C7(4096) D0(4096) FA(4096)
4  5/ 13  E8(5120) 1D(4608) 25(4608) 6C(4608) A3(4608) BB(4608) D5(4608) F7(4608) 31(4352) 3C(4352) 42(4352) 8D(4352) C3(4352)

Failed. Next try with 5000 IVs.

```

Gambar 4.5 Hasil Akhir Pengujian ke 5

Pada gambar 4.6 adalah hasil akhir pengujian pada metode WEP

```

Aircrack-ng 1.5.2
[00:00:03] Tested 127401 keys (got 5406 IVs)

KB  depth  byte(vote)
0  23/ 32  F7(7424) 1B(7168) 25(7168) 3F(7168) 4E(7168) 74(7168) 94(7168) AF(7168) C1(7168) 1E(6912) 32(6912) 6C(6912) 75(6912)
1  27/  1  EA(6912) 0D(6656) 19(6656) 27(6656) 49(6656) 64(6656) 69(6656) 6E(6656) 74(6656) 8C(6656) B0(6656) B1(6656) 20(6400)
2  9/  2   41(7680) 0E(7424) 20(7424) 63(7424) A9(7424) E6(7424) 11(7168) 5B(7168) 68(7168) 7E(7168) 83(7168) 92(7168) AB(7168)
3  4/ 20  AA(7936) 08(7680) 45(7680) 6E(7680) 92(7680) B5(7680) CC(7680) 44(7424) 62(7424) 70(7424) 8B(7424) AE(7424) D3(7424)
4  4/ 16  43(7936) D7(7680) F0(7680) FD(7680) 09(7424) 25(7424) 94(7424) AE(7424) B5(7424) DF(7424) E5(7424) F3(7424) 54(7168)

Failed. Next try with 10000 IVs.

```

Gambar 4.6 Hasil Akhir Pengujian ke 6

Pada gambar 4.7 adalah hasil akhir pengujian pada metode WEP

```

Aircrack-ng 1.5.2

[00:00:07] Tested 149473 keys (got 10134 IVs)

KB  depth  byte(vote)
0  17/ 18  FC(13056) 27(12800) 2E(12800) 3A(12800) 4E(12800) 57(12800) 81(12800) C8(12800) 0A(12544) 2A(12544) FB(12544) 34(12288) 84(12288)
1  32/  1  FA(12288) 41(12032) 47(12032) 6F(12032) 8F(12032) D6(12032) 1D(11776) 8D(11776) BE(11776) CA(11776) DB(11776) FD(11776) 22(11520)
2  14/ 28  B3(13056) 23(12800) 45(12800) 47(12800) 5B(12800) 69(12800) B7(12800) 3C(12544) 80(12544) 8A(12544) 43(12288) 46(12288) 95(12288)
3  1/ 10  C8(15360) 02(14080) 49(14080) 5F(14080) 31(13824) 87(13824) 92(13824) A5(13824) 0D(13568) FE(13568) 10(13312) 33(13056) AC(13056)
4  27/  4  CF(12032) 1D(11776) 2F(11776) 52(11776) 7D(11776) 9A(11776) B9(11776) BC(11776) DC(11776) 13(11520) 1A(11520) 3B(11520) 42(11520)

Failed. Next try with 15000 IVs.

```

Gambar 4.7 Hasil Akhir Pengujian ke 7

Pada gambar 4.8 adalah hasil akhir pengujian pada metode WEP

```

Aircrack-ng 1.5.2

[00:00:07] Tested 175321 keys (got 15201 IVs)

KB  depth  byte(vote)
0  9/ 10  68(19456) 2B(19200) 73(19200) D5(19200) 1F(18688) 34(18688) 44(18688) C4(18688) F7(18688) 0A(18432) 2D(18432) 32(18432) 3D(18432)
1  12/ 13  E1(18432) 86(18176) 02(17920) 22(17920) 2A(17920) 4F(17920) 8D(17920) 0E(17664) 45(17664) 5D(17664) 79(17664) 7E(17664) A2(17664)
2  10/ 13  77(18944) 2C(18688) 8B(18688) E3(18688) F7(18688) 55(18432) A5(18432) C1(18432) 75(18176) 78(18176) DC(18176) 0E(17920) 54(17920)
3  14/  3  CC(18944) 12(18688) 14(18688) 15(18688) 75(18688) 7C(18432) D4(18432) 36(18176) 78(18176) 32(17920) 42(17920) 68(17920) E2(17920)
4  9/  4  9A(18432) 79(18176) 95(18176) FF(18176) 51(17920) 66(17920) 83(17920) A8(17920) B4(17920) B8(17920) C9(17920) CC(17920) E7(17920)

Failed. Next try with 20000 IVs.

```

Gambar 4.8 Hasil Akhir Pengujian ke 8

Pada gambar 4.9 adalah hasil akhir pengujian pada metode WEP

```

Aircrack-ng 1.5.2

[00:00:00] Tested 0 keys (got 2 IVs)

KB  depth  byte(vote)
0  255/256  FF(  0) 5E( 256) 00(  0) 01(  0) 02(  0) 03(  0) 04(  0) 05(  0) 06(  0) 07(  0) 08(  0) 09(  0) 0A(  0)
1  1/  4  B2( 256) 00(  0) 01(  0) 02(  0) 03(  0) 04(  0) 05(  0) 06(  0) 07(  0) 08(  0) 09(  0) 0A(  0) 0B(  0)
2  1/  2  E2( 256) 00(  0) 01(  0) 02(  0) 03(  0) 04(  0) 05(  0) 06(  0) 07(  0) 08(  0) 09(  0) 0A(  0) 0B(  0)
3  1/  3  8F( 256) 00(  0) 01(  0) 02(  0) 03(  0) 04(  0) 05(  0) 06(  0) 07(  0) 08(  0) 09(  0) 0A(  0) 0B(  0)
4  1/  4  99( 256) 00(  0) 01(  0) 02(  0) 03(  0) 04(  0) 05(  0) 06(  0) 07(  0) 08(  0) 09(  0) 0A(  0) 0B(  0)

Failed. Next try with 5000 IVs.
^[[A

```

Gambar 4.9 Hasil Akhir Pengujian ke 9

Pada gambar 4.10 adalah hasil akhir pengujian pada metode WEP

```

Aircrack-ng 1.5.2
[00:00:05] Tested 139777 keys (got 3995 IVs)

KB depth byte(vote)
0 11/ 13 82(5888) 57(5632) 59(5632) A9(5632) B0(5632) B0(5632) E6(5632) F9(5632) 16(5376) 24(5376) B2(5376) B9(5376) C8(5376)
1 29/ 1 E2(5376) 31(5120) 32(5120) 33(5120) 3E(5120) 95(5120) B6(5120) C0(5120) D7(5120) E4(5120) 0F(4864) 18(4864) 35(4864)
2 1/ 10 CE(7168) 91(6656) 05(6400) 30(6400) 74(6400) ED(6400) 13(6144) 25(6144) 33(6144) 26(5888) 61(5888) 6C(5888) 2E(5632)
3 25/ 3 E8(5376) 22(5120) 29(5120) 2D(5120) 2E(5120) 33(5120) 41(5120) 49(5120) 53(5120) 57(5120) 6C(5120) 6F(5120) 7B(5120)
4 20/ 53 AB(5632) 04(5376) 12(5376) 39(5376) 4E(5376) 6F(5376) 80(5376) A6(5376) B7(5376) D8(5376) E4(5376) 2B(5120) 2E(5120)

Failed. Next try with 5000 IVs.

```

Gambar 4.10 Hasil Akhir Pengujian ke 10

Pada gambar 4.11 adalah hasil akhir pengujian pada metode WEP

```

Aircrack-ng 1.5.2
[00:00:05] Tested 163747 keys (got 16324 IVs)

KB depth byte(vote)
0 5/ 7 6A(20736) 40(20224) 54(20224) 76(20224) 8B(20224) 47(19968) F9(19712) FF(19712) 39(19456) 74(19456) AE(19456) B5(19456) BA(19456)
1 103/104 84(16896) 15(16640) 58(16640) 98(16640) C3(16640) E3(16640) FC(16640) 0A(16384) 11(16384) 23(16384) 27(16384) 39(16384) 47(16384)
2 40/ 2 D8(18432) 00(18176) 09(18176) 1F(18176) 3B(18176) 3E(18176) 40(18176) A5(18176) AE(18176) B6(18176) C2(18176) DF(18176) 15(17920)
3 1/ 4 27(22016) 34(21760) 3E(21760) 40(21504) 4F(21248) C7(21248) 90(20992) 24(20480) 33(20224) 53(20224) 5E(20224) 75(20224) 8D(20224)
4 55/ 4 E1(17920) 0B(17664) 24(17664) 3E(17664) 42(17664) 4C(17664) 61(17664) 73(17664) 7F(17664) 87(17664) A0(17664) B2(17664) B5(17664)

Failed. Next try with 20000 IVs.

```

Gambar 4.11 Hasil Akhir Pengujian ke 11

Pada gambar 4.12 adalah hasil akhir pengujian pada metode WEP

```

Aircrack-ng 1.5.2
[00:00:04] Tested 166141 keys (got 92 IVs)

KB depth byte(vote)
0 15/ 65 FF( 512) 03( 256) 10( 256) 14( 256) 15( 256) 20( 256) 24( 256) 26( 256) 32( 256) 37( 256) 39( 256) 41( 256) 48( 256)
1 12/ 13 1F( 512) 00( 256) 12( 256) 1A( 256) 1B( 256) 24( 256) 27( 256) 30( 256) 39( 256) 3C( 256) 42( 256) 43( 256) 45( 256)
2 1/ 2 A6( 768) 03( 512) 05( 512) 06( 512) 24( 512) 4B( 512) 78( 512) 83( 512) C4( 512) D0( 512) 00( 256) 08( 256) 0D( 256)
3 77/ 3 FD( 256) 00( 0) 01( 0) 02( 0) 03( 0) 04( 0) 06( 0) 07( 0) 08( 0) 0B( 0) 0C( 0) 0E( 0) 0F( 0)
4 12/ 4 C4( 512) 03( 256) 07( 256) 0B( 256) 0D( 256) 17( 256) 1B( 256) 1D( 256) 1E( 256) 1F( 256) 21( 256) 36( 256) 3B( 256)

Failed. Next try with 5000 IVs.

```

Gambar 4.12 Hasil Akhir Pengujian ke 12

Pada gambar 4.13 adalah hasil akhir pengujian pada metode WEP

```

Aircrack-ng 1.5.2

[00:00:06] Tested 167617 keys (got 9270 IVs)

KB  depth  byte(vote)
0  10/ 12  14(12544) 34(12288) 3A(12032) 49(12032) 7C(12032) ED(11776) 17(11520) 3C(11520) 57(11520) 9F(11520) B4(11520) E5(11520) 09(11264)
1  31/ 36  CD(11264) 07(11008) 18(11008) A6(11008) DA(11008) 20(10752) 2A(10752) 81(10752) 91(10752) 9F(10752) BA(10752) BD(10752) CC(10752)
2  3/ 4  6A(13824) 09(13056) 19(13056) 11(12800) A2(12800) CD(12544) DA(12544) F8(12544) 14(12288) 23(12288) 53(12288) 5E(12032) 8F(12032)
3  28/ 3  EF(11264) 1E(11008) 24(11008) 26(11008) 33(11008) 50(11008) 6B(11008) A1(11008) AB(11008) B1(11008) DA(11008) E4(11008) 13(10752)
4  16/ 4  EE(11776) 55(11520) 6D(11520) 70(11520) D8(11520) F9(11520) FB(11520) 0D(11264) 29(11264) 30(11264) 7D(11264) 88(11264) D6(11264)

Failed. Next try with 10000 IVs.

```

Gambar 4.13 Hasil Akhir Pengujian ke 13

Pada gambar 4.14 adalah hasil akhir pengujian pada metode WEP

```

Aircrack-ng 1.5.2

[00:00:09] Tested 175755 keys (got 18189 IVs)

KB  depth  byte(vote)
0  1/ 2  0E(26112) 79(23552) A6(23296) D3(22784) 0A(22528) B2(22528) DF(22528) FB(22016) FF(22016) 16(21760) 48(21760) F8(21760) 1F(21504)
1  26/ 27  EF(20992) 0A(20736) 1D(20736) 2E(20736) 6D(20736) 8A(20736) 9E(20736) F1(20736) FA(20736) 01(20480) 05(20480) 15(20480) 47(20480)
2  26/ 31  F2(20992) 13(20736) 15(20736) E2(20736) E8(20736) 29(20480) 44(20480) 73(20480) 7B(20480) B1(20480) B8(20480) FE(20480) 1C(20224)
3  24/ 3  F9(21248) 1C(20992) 28(20992) 56(20992) 67(20992) 25(20736) 44(20736) 82(20736) 9D(20736) CA(20736) E1(20736) 08(20480) 1D(20480)
4  54/ 4  E5(19968) 15(19712) 2A(19712) 46(19712) 65(19712) 75(19712) C1(19712) C5(19712) E7(19712) F2(19712) 06(19456) 0E(19456) 16(19456)

Failed. Next try with 20000 IVs.

```

Gambar 4.14 Hasil Akhir Pengujian ke 14

Pada gambar 4.15 adalah hasil akhir pengujian pada metode WEP

```

TP-LINK Aircrack-ng 1.5.2

[00:00:10] Tested 156277 keys (got 133 IVs)

KB  depth  byte(vote)
0  107/108  F9( 256) 00( 0) 01( 0) 02( 0) 03( 0) 04( 0) 05( 0) 09( 0) 0A( 0) 0C( 0) 0D( 0) 0E( 0) 11( 0)
1  4/ 23  D8( 768) 00( 512) 0E( 512) 2A( 512) 2F( 512) 51( 512) 56( 512) 63( 512) 71( 512) 8F( 512) 94( 512) 9E( 512) B3( 512)
2  30/ 2  FC( 512) 02( 256) 06( 256) 07( 256) 09( 256) 0D( 256) 14( 256) 1D( 256) 1F( 256) 20( 256) 21( 256) 24( 256) 25( 256)
3  0/ 2  2C(1280) 77( 768) E0( 768) 08( 512) 09( 512) 1F( 512) 37( 512) 45( 512) 57( 512) 5D( 512) 5E( 512) 60( 512) 73( 512)
4  1/ 4  AB( 768) 00( 512) 06( 512) 0A( 512) 14( 512) 18( 512) 1C( 512) 26( 512) 28( 512) 2E( 512) 32( 512) 33( 512) 35( 512)

Failed. Next try with 5000 IVs. WEP

```

Gambar 4.15 Hasil Akhir Pengujian ke 15

Pada gambar 4.16 adalah hasil akhir pengujian yang berhasil pada metode WEP

```

Aircrack-ng 1.5.2

[00:00:00] Tested 2 keys (got 49545 IVs)

KB depth byte(vote)
0 0/ 1 55(69632) 5B(58880) E7(58112) 79(57600) 0E(57344) 34(57344) 7C(57088) B4(57088) 04(56832) 2E(56576) 36(56576) 3C(56576) CE(56576)
1 0/ 1 69(69632) 6A(61440) 93(60416) 88(58624) 44(57344) 23(56832) 5C(56576) 8E(56576) 8B(56064) A5(55808) AE(55552) 46(55296) 5F(55296)
2 0/ 1 72(60160) F6(59904) 13(59648) 29(59392) 93(57856) 8D(57344) 1F(57088) 31(56832) 63(56576) 02(56320) 33(56064) AB(56064) 4D(55808)
3 0/ 1 75(65024) 66(60672) 35(58368) 36(57856) CE(57856) 2B(57344) 0E(56832) BE(56832) 83(55808) C1(55552) C4(55552) E3(55552) 56(55296)
4 0/ 1 6E(68608) 6E(59648) AF(59392) 01(58368) DE(57600) 49(57344) 7B(57344) 89(57344) 1A(56576) 44(56320) BD(56320) EA(56064) 31(55808)
5 0/ 1 67(65280) 0E(58624) 9B(57600) 4A(57088) F7(56832) 60(56576) 29(56064) 28(55808) 6E(55808) 16(55552) 8F(55552) 45(55296) F1(55296)
6 0/ 1 67(70144) 52(60160) B9(57088) 80(56832) 89(56576) B2(56576) BE(56576) C0(56576) 0A(56320) 46(55552) 4F(55552) DF(55552) 05(55296)
7 0/ 1 75(65280) 7B(59136) 82(58112) 11(57600) 4A(56576) CF(56576) 33(56320) 3E(56320) 4E(56320) 62(56064) C2(56064) F5(55808) 6B(55040)
8 0/ 1 6C(62720) C1(58624) F3(58368) BA(57856) DA(57088) 07(56576) 00(55808) 33(55552) 73(55552) 12(55296) AF(55296) DD(55296) 34(55040)
9 0/ 1 32(62976) 59(59136) 45(58368) 53(58112) 6F(57600) CB(57344) 56(57088) 92(57088) 99(56832) 7D(56576) 93(56576) DF(56320) E9(56320)
10 0/ 1 30(66816) A2(59648) 81(58112) 3A(57344) 89(57344) 49(57088) 9D(56576) CA(56576) 34(56320) 10(56064) D1(56064) 03(55808) 7A(55808)
11 0/ 1 32(64000) 13(61184) 33(60160) 7D(60160) 14(59136) 1B(57600) 4B(57600) 20(57088) 9E(56832) DE(56832) 01(56576) 36(56576) 00(56320)
12 0/ 1 30(67584) 7E(61952) 16(58368) 09(57600) F6(57344) 92(57088) 46(56832) 05(56576) B9(56576) D1(56576) 15(56320) 2E(56320) BC(56320)

KEY FOUND! [ 55:69:72:75:6E:67:67:75:6C:32:30:32:30 ] (ASCII: UirungguL2020 )
Decrypted correctly: 100%

```

Gambar 4.16 Hasil Akhir Pengujian ke 16

4.3 Hasil Akhir Pengujian Metode WPA-PSK

Pengujian terhadap metode WPA-PSK tersebut akan dilakukan pengujian sebanyak 20 kali pengujian gagal dan 1 pengujian akhir yang benar total pengujian pada WPA-PSK sebanyak 21 pengujian.

Pada gambar 4.17 adalah hasil akhir pengujian pada metode WPA-PSK

```

Aircrack-ng 1.5.2

[00:12:13] 488133/488132 keys tested (382.03 k/s)

Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~# █
Master Key : 24 92 54 E5 A5 11 21 EE D8 79 FF 60 5E 75 10 EF
             B0 62 13 A6 AF 64 41 E1 A7 2E DF 21 EF C0 5E CC

Transient Key : 2B 94 FF 9C 9C F4 B0 C5 54 47 96 F5 7A 3E DA BF
                A5 77 D0 A0 83 32 EE 7A 4F 9B EE F6 F2 44 85 D5
                03 C1 8A 7E 29 89 7A 8C BD 0E 40 76 E5 02 3F 7B
                19 C9 D6 BB C0 53 C7 43 2E 8D 91 1C AA 30 E8 3F

EAPOL HMAC : 79 41 D8 65 26 4D E2 2F F4 F8 5A A3 B8 8F F9 DA

WPA-PSK/WPA2-PSK

```

Gambar 4.17 Hasil Akhir Pengujian ke 1

Pada gambar 4.18 adalah hasil akhir pengujian pada metode WPA-PSK

```

Aircrack-ng 1.5.2
[00:11:40] 488133/488132 keys tested (381.36 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~#
Master Key : 2E C7 E7 F3 80 EE 37 0B 56 FE 79 BD 50 D3 DB 02
            00 DF 93 36 7F D0 0E D7 79 E4 A5 89 09 F7 36 57

Transient Key : 0E 3A EC A7 83 22 4A A0 3F 29 81 9E E3 12 C7 3F
                D8 71 BE DF 47 A0 2C 05 36 C6 35 B7 B5 E7 ED 42
                02 D6 CB 96 D7 55 70 F5 86 42 26 15 C6 D6 01 8F
                DA 25 DA 73 E6 B4 AE FD 5E 9E B5 60 6C AA 25 EE

EAPOL HMAC : 14 E8 3E E0 A6 E0 D0 0F 85 28 40 3D 9B 76 CD 15

```

Gambar 4.18 Hasil Akhir Pengujian ke 2

Pada gambar 4.19 adalah hasil akhir pengujian pada metode WPA-PSK

```

Aircrack-ng 1.5.2
[00:11:26] 488133/488132 keys tested (382.24 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~#
Master Key : 8A 27 F4 2B F5 1E 2D 06 98 D3 93 74 38 93 60 9D
            76 2D BF A6 4E C8 BB 96 D3 95 45 E6 D6 1F B5 2E

Transient Key : 24 FB 8A 59 B5 6B BB 26 99 3E 72 B1 57 26 26 CA
                FB E8 BD 02 D9 03 B0 B6 88 36 46 F4 25 C7 2F 24
                C0 DB EA 89 47 0F D7 C6 32 65 F2 49 7B F6 BF C9
                51 6D 62 36 84 77 E9 85 35 05 46 FA B3 0F 3D 19

EAPOL HMAC : 69 3C CD B3 C9 58 8A F6 A5 29 DB 96 CE 71 BB E0

```

Gambar 4.19 Hasil Akhir Pengujian ke 3

Pada gambar 4.20 adalah hasil akhir pengujian pada metode WPA-PSK

```

Aircrack-ng 1.5.2

[00:11:40] 488133/488132 keys tested (379.63 k/s)

Time left: 0 seconds                               100.00%

KEY NOT FOUND

root@Skripsi:~# █
Master Key      : C9 2F 62 C9 B2 76 51 9C 73 FA 29 31 BF 06 0A 8E
                  31 46 2E 9E F4 62 E6 43 CF FC 83 FA 82 96 8D DA

Transient Key   : EA D4 E2 B0 B6 92 7B 8D B7 02 EB 58 1F 78 88 E6
                  58 37 D3 03 02 FC 6B CB 4B 2F D0 6A 0F 2C 24 85
                  9A 80 34 A1 40 8D D5 5F 62 71 07 B7 47 03 C5 E4
                  B4 F2 C0 43 E9 37 D5 F7 97 2E A2 00 E4 14 EF 5C

EAPOL HMAC     : C5 A8 36 8C 3D 7E F0 BF F1 5C DD 30 80 A1 40 23

```

Gambar 4.20 Hasil Akhir Pengujian ke 4

Pada gambar 4.21 adalah hasil akhir pengujian pada metode WPA-PSK

```

Aircrack-ng 1.5.2

[00:11:54] 488133/488132 keys tested (345.66 k/s)

Time left: 0 seconds                               100.00%

KEY NOT FOUND

root@Skripsi:~# █
Master Key      : 24 92 54 E5 A5 11 21 EE D8 79 FF 60 5E 75 10 EF
                  B0 62 13 A6 AF 64 41 E1 A7 2E DF 21 EF C0 5E CC

Transient Key   : C2 32 09 DA 58 6A 53 28 95 F7 1C AE 77 03 19 6C
                  2A 8F 6F 86 C3 EF B3 CB D9 D3 30 73 5E 08 F4 1A
                  7B 85 80 73 20 31 60 65 9C 50 D3 04 B3 80 30 E2
                  DD BE 84 E1 03 33 94 5D 0E BD C2 8C 34 52 18 CE

EAPOL HMAC     : AB AC D9 19 75 4C F3 E1 36 50 AE 13 0A 5D 92 77

```

Gambar 4.21 Hasil Akhir Pengujian ke 5

Pada gambar 4.22 adalah hasil akhir pengujian pada metode WPA-PSK

```

Aircrack-ng 1.5.2

[00:11:30] 488133/488132 keys tested (382.15 k/s)

Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~#
root@Skripsi:~# : EB 34 07 03 E2 C5 88 A8 03 74 EF D1 B4 05 74 4E
                  03 20 BA 23 27 D7 27 33 FC 3B D3 33 D4 C4 8F FA

Transient Key : 19 45 23 37 E4 82 DD 41 1B E8 63 9C 5E 31 2D 83
                5F 23 E4 90 35 DE 9E 69 4D D2 B9 56 9A 8D CF BC
                FA 69 99 26 C7 71 7C 8A 41 BD 9E 8D 40 9C B8 97
                35 84 03 9F 2E 12 FD D2 13 F3 F9 4B 67 12 1F 3D

EAPOL HMAC : B4 C4 2C C8 79 C6 E8 0F 3E 56 DC 3C 2A 64 34 5C

```

Gambar 4.22 Hasil Akhir Pengujian ke 6

Pada gambar 4.23 adalah hasil akhir pengujian pada metode WPA-PSK

```

Aircrack-ng 1.5.2

[00:11:42] 488133/488132 keys tested (381.33 k/s)

Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~#
root@Skripsi:~# : C9 2F 62 C9 B2 76 51 9C 73 FA 29 31 BF 06 0A 8E
                  31 46 2E 9E F4 62 E6 43 CF FC 83 FA 82 96 8D DA

Transient Key : 7C E5 CF 53 D6 47 81 C3 73 D3 A8 D6 79 45 FE 03
                8C E8 F7 22 B7 32 CD 29 D7 AE 72 F0 66 E3 83 CC
                72 C8 FD 0B 1E FD 98 36 F6 B7 19 88 B5 D1 F7 75
                18 E4 20 45 C0 2C CC 5F 1D 99 32 4C F5 0E AF 20

EAPOL HMAC : 1D 5D 43 52 1E B4 73 81 0B 89 34 CB 5D 98 FD 3F

```

Gambar 4.23 Hasil Akhir Pengujian ke 7

Pada gambar 4.24 adalah hasil akhir pengujian pada metode WPA-PSK

```

Aircrack-ng 1.5.2

[00:12:30] 488133/488132 keys tested (374.96 k/s)

Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~# █
Master Key      : 27 63 B3 7A 01 39 19 9B D4 70 11 74 D1 E1 8C 09
                  52 00 AF 71 82 37 3D D3 C2 65 23 86 95 7D 96 1C

Transient Key   : 87 08 C2 9F 32 95 4E 6A 84 AC F4 28 F0 14 72 4B
                  CA C8 D2 8F DD 69 24 30 9E 1D E2 F3 84 0C AD DB
                  FD 6F 46 48 DC 87 E6 CB 7C 63 5F A4 9E D2 F1 1A
                  13 2A FB 6F 0F B6 49 89 54 05 B0 CD 11 7C BB 86

EAPOL HMAC     : 80 9D 1E 73 A7 04 5F 66 22 BE 8B 30 55 79 A9 B7
  
```

Gambar 4.24 Hasil Akhir Pengujian ke 8

Pada gambar 4.25 adalah hasil akhir pengujian pada metode WPA-PSK

```

Aircrack-ng 1.5.2

[00:12:27] 488133/488132 keys tested (368.06 k/s)

Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~# █
Master Key      : 6A F8 DC FD 18 16 CB 59 9E 1D A7 98 99 D5 1C 33
                  40 31 3F F2 18 F0 F1 25 9C EF 80 D7 64 F5 51 BA

Transient Key   : 02 E9 10 53 E9 67 6C 6E 8B 13 7C 6D 49 F3 E7 31
                  00 D4 0B F7 CD CA 3F 55 15 20 EC 6B 05 5E 72 28
                  BE 0D 8D 5E 06 07 C5 22 21 94 50 63 FC B2 D2 FC
                  AD DE 14 99 97 2D A1 C9 8D D9 EC CA 3C 31 19 21

EAPOL HMAC     : 76 DF A8 6B 8D 57 37 A0 39 F5 3D F1 5B AA 0F 84
  
```

Gambar 4.25 Hasil Akhir Pengujian ke 9

Pada gambar 4.26 adalah hasil akhir pengujian pada metode WPA-PSK

```
Aircrack-ng 1.5.2
[00:13:06] 488133/488132 keys tested (367.66 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~#
Master Key      : 1E 33 AD AA 16 ED 0F 21 0F 13 91 70 DC 70 FD 65
                  6E 8E 67 45 69 43 A9 EE 43 53 97 A2 DC 7A 97 2E
Transient Key   : 4C 6F CC E8 F6 98 08 99 1E 38 00 17 8B 2E 8B F5
                  4A A8 04 FC 13 FE B6 D6 DC DD E4 D7 89 1B 40 8D
                  80 48 A2 B1 C8 1C E4 45 F3 F9 CD 0E BF 83 44 C8
                  55 68 38 73 63 29 20 12 B9 60 B5 4D 9C AB F5 0F
EAPOL HMAC     : 9B A3 B9 8B F9 D7 E2 34 39 F7 21 4D 93 FC B4 48
```

Gambar 4.26 Hasil Akhir Pengujian ke 10

Pada gambar 4.27 adalah hasil akhir pengujian pada metode WPA-PSK

```
root@Skripsi:~# aircrack-ng -w p.txt revisi8-01.cap
Opening revisi8-01.cape wait ...
Read 6185 packets.

# BSSID          ESSID          Encryption
1  10:FE:ED:2F:F2:52  TP-LINK_2FF252  WPA (1 handshake)

Choosing first network as target.

Opening revisi8-01.cape wait ...
Read 6185 packets.

1 potential targets
```

Gambar 4.27 Hasil Akhir Pengujian ke 11

Pada gambar 4.28 adalah hasil akhir pengujian pada metode WPA-PSK

```

DEVICES
Aircrack-ng 1.5.2
[00:12:33] 488133/488132 keys tested (378.55 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
PLACES
root@Skripsi:~# █
Master Key : C9 2F 62 C9 B2 76 51 9C 73 FA 29 31 BF 06 0A 8E
              31 46 2E 9E F4 62 E6 43 CF FC 83 FA 82 96 8D DA
Transient Key : 54 67 F9 58 A1 73 18 96 6E 00 7A 34 CD C3 42 B1
              DD 85 AB C3 66 4A 2D B7 5E 25 6D 4C 32 3A CF 6E
              07 08 B3 FA F7 FD 38 9A CB BD 82 2D C9 87 D3 93
              7D 2A 05 B1 D5 AE 90 ED 9C 1B 49 AC B2 05 61 08
EAPOL HMAC : 20 2D E1 0D F7 C6 E7 20 D0 2C 92 F2 D7 27 94 E5
  
```

Gambar 4.28 Hasil Akhir Pengujian ke 12

Pada gambar 4.29 adalah hasil akhir pengujian pada metode WPA-PSK

```

DEVICES
Aircrack-ng 1.5.2
[00:13:42] 488133/488132 keys tested (369.70 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
PLACES
root@Skripsi:~# █
Master Key : 8A 27 F4 2B F5 1E 2D 06 98 D3 93 74 38 93 60 9D
              76 2D BF A6 4E C8 BB 96 D3 95 45 E6 D6 1F B5 2E
Transient Key : 53 91 75 19 73 33 52 8F 63 F7 FA 5A 27 60 48 67
              82 02 94 0D F3 D3 98 A4 D3 63 3C 61 B1 3B A2 7F
              DF C7 C5 CB 45 08 17 88 4D 1D 7D 06 77 0A 56 78
              08 0B 61 7A BC 37 01 1B 3C 5B 1E 48 8A 6B 68 13
EAPOL HMAC : 45 A8 27 4A 2B 04 3A 8B BD E3 4A D1 BF D0 15 C9
  
```

Gambar 4.29 Hasil Akhir Pengujian ke 13

Pada gambar 4.30 adalah hasil akhir pengujian pada metode WPA-PSK

```

Aircrack-ng 1.5.2

[00:11:30] 488133/488132 keys tested (382.15 k/s)

Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~#
root@Skripsi:~# : EB 34 07 03 E2 C5 88 A8 03 74 EF D1 B4 05 74 4E
                  03 20 BA 23 27 D7 27 33 FC 3B D3 33 D4 C4 8F FA

Transient Key : 19 45 23 37 E4 82 DD 41 1B E8 63 9C 5E 31 2D 83
                5F 23 E4 90 35 DE 9E 69 4D D2 B9 56 9A 8D CF BC
                FA 69 99 26 C7 71 7C 8A 41 BD 9E 8D 40 9C B8 97
                35 84 03 9F 2E 12 FD D2 13 F3 F9 4B 67 12 1F 3D

EAPOL HMAC : B4 C4 2C C8 79 C6 E8 0F 3E 56 DC 3C 2A 64 34 5C

```

Gambar 4.30 Hasil Akhir Pengujian ke 14

Pada gambar 4.31 adalah hasil akhir pengujian pada metode WPA-PSK

```

Aircrack-ng 1.5.2

[00:12:32] 488133/488132 keys tested (380.71 k/s)

Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~#
root@Skripsi:~# Master Key : 55 60 AF F0 37 78 C4 20 8F C9 77 A8 B3 8F AD 68
                  88 26 8B 88 3F 10 BA D1 20 BF 25 B9 2C 5E 39 2B

Transient Key : 28 83 45 44 7F 39 7E 34 78 45 ED 60 1E 6F 34 7D
                FA B3 8E AE A9 DF 0D 3D F7 F3 C5 08 5A EB 6F F9
                C1 34 C7 B0 62 0A 29 03 C4 94 67 71 DF F8 79 E3
                A7 0F 8A D9 48 7E 45 24 0F FA CC C1 5C 23 3A 25

EAPOL HMAC : C9 B1 1E 25 58 D8 E6 E5 AB 54 2B 5D 5A E1 82 1D

```

Gambar 4.31 Hasil Akhir Pengujian ke 15

Pada gambar 4.32 adalah hasil akhir pengujian pada metode WPA-PSK

```

Aircrack-ng 1.5.2

[00:16:07] 488133/488132 keys tested (381.23 k/s)
Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~#
Master Key      : 1E 33 AD AA 16 ED 0F 21 0F 13 91 70 DC 70 FD 65
                  6E 8E 67 45 69 43 A9 EE 43 53 97 A2 DC 7A 97 2E

Transient Key   : 2E 2F 71 5F 9C 4E A5 B9 ED FB 07 0C 38 FD A0 AE
                  A2 8C 10 F2 49 F8 8E 79 3F 4D EC B9 16 C9 EF 5E
                  DC 31 86 8D 6F BE 14 B0 BB 77 A5 63 5B 95 D1 92
                  27 25 06 C1 D7 19 BD E9 D0 F6 12 43 57 7D 67 45

EAPOL HMAC     : 62 36 A8 45 8B 8E A5 B6 0C 6F 94 0F 32 BF 21 A5

```

Gambar 4.32 Hasil Akhir Pengujian ke 16

Pada gambar 4.33 adalah hasil akhir pengujian pada metode WPA-PSK

```

Aircrack-ng 1.5.2

[00:11:43] 488133/488132 keys tested (379.52 k/s)
Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~#
Master Key      : CE 3F 67 41 D5 6E EC A2 D8 66 40 F0 77 01 11 54
                  94 00 7D 52 7C C5 2C 14 E8 B6 E3 DA CD A6 01 1A

Transient Key   : 40 28 28 28 2E DC C8 85 6A B6 7E BF 75 2B 6F 48
                  18 2B 8D 82 56 ED 78 78 26 54 21 91 1A A7 2E CC
                  43 A8 43 EB EE 9D F5 C1 FC DC 42 E1 AD DF F4 82
                  EE F9 BF 8E D8 B4 5A 4D FB 5A 4D 31 83 88 F4 5E

EAPOL HMAC     : 34 9E AD 96 85 A0 E0 4B D2 42 E4 72 E9 78 CF 90

```

Gambar 4.33 Hasil Akhir Pengujian ke 17

Pada gambar 4.34 adalah hasil akhir pengujian pada metode WPA-PSK

```

Aircrack-ng 1.5.2

[00:20:45] 488133/488132 keys tested (376.55 k/s)

Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~#
Master Key      : AF D8 D3 5A 24 9C DC 56 8A 5A 1F 0F A2 CD 41 39
                  02 D8 EF EE 2F D1 7E 31 8A 6E 33 17 FE 46 4C 53

Transient Key   : 73 8D 6E 42 18 16 09 8E CD 89 0A 65 BB FB B1 5A
                  F0 61 D4 FA 01 7C 0D 90 40 9B 7D B8 57 50 4F 97
                  C2 B5 10 44 18 94 DF 57 C6 6F BD 64 73 25 AC 11
                  2E 53 67 66 9E 9A F3 FB 46 A9 DB 0D A1 E3 29 3E

EAPOL HMAC     : C4 C1 A9 FA C6 7A 0F E0 49 66 60 FB E1 42 D8 F4

```

Gambar 4.34 Hasil Akhir Pengujian ke 18

Pada gambar 4.35 adalah hasil akhir pengujian pada metode WPA-PSK

```

Aircrack-ng 1.5.2

[00:11:34] 488133/488132 keys tested (381.46 k/s)

Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~#
Master Key      : C9 2F 62 C9 B2 76 51 9C 73 FA 29 31 BF 06 0A 8E
                  31 46 2E 9E F4 62 E6 43 CF FC 83 FA 82 96 8D DA

Transient Key   : FE 27 60 53 78 83 B3 64 F2 06 C6 48 54 19 8E 04
                  13 3B DD F7 DC A6 22 52 83 29 A9 85 B3 CD F8 A6
                  41 45 BB DD 2F 9C 12 06 01 4A B6 61 A8 46 23 DB
                  B5 01 10 44 8A D6 9D DE 98 C1 D4 26 78 11 CA 3E

EAPOL HMAC     : 85 12 B6 F8 71 E2 0B D5 EE B5 85 14 90 A8 7B B3

```

Gambar 4.35 Hasil Akhir Pengujian ke 19

Pada gambar 4.36 adalah hasil akhir pengujian pada metode WPA-PSK

```

TP-LINK
Status: Aircrack-ng 1.5.2
[00:11:41] 488133/488132 keys tested (348.30 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~#
Master Key : 8A 27 F4 2B F5 1E 2D 06 98 D3 93 74 38 93 60 9D
              76 2D BF A6 4E C8 BB 96 D3 95 45 E6 D6 1F B5 2E
Transient Key : 59 3C 50 B5 2D 13 C4 A4 00 A3 0A E5 8C 31 43 CD
                 33 60 5A F9 CC 18 CB 92 22 5B E2 AC 4B F0 C8 7E
                 C2 EB 15 EC 26 5D 2E A7 65 E7 FD DD 4D B0 F8 2E
                 33 15 2A F7 E1 53 EB 1F 05 7B AD A3 D8 3D 4D 1E
  
```

Gambar 4.36 Hasil Akhir Pengujian ke 20

Pada gambar 4.37 adalah hasil akhir pengujian yang berhasil pada metode WPA-PSK

```

Aircrack-ng 1.5.2
[00:00:14] 10663/488132 keys tested (632.52 k/s)
Time left: 12 minutes, 35 seconds 2.18%
KEY FOUND! [ Uirunggul2020 ]
Master Key : CC C2 F0 F0 3E BC 38 A6 A9 59 58 EA 3D 49 D2 33
              7F D8 65 B9 2B 35 EB A6 63 6F B9 02 04 80 94 7C
Transient Key : 16 A5 A7 A7 98 5D 40 63 AC 76 10 99 4D 04 72 5F
                 87 91 06 87 BE 08 8B AE CC 59 C3 8D CE 2A 9A 5C
                 58 0A 05 25 75 2F F1 FC D5 92 DC F1 24 4A 03 C8
                 24 4E 90 94 35 37 7B F5 0A 2F 2A 89 F4 30 40 D4
EAPOL HMAC : 97 E5 D7 62 A5 B1 2B 07 3A 9A 26 5F F4 87 2D BA
root@Skripsi:~#
  
```

Gambar 4.37 Hasil Akhir Pengujian ke 21

4.4 Hasil Akhir Pengujian Metode WPA2-PSK

Pengujian terhadap metode WPA2-PSK tersebut akan dilakukan pengujian sebanyak 25 kali pengujian gagal dan 1 pengujian akhir yang benar total pengujian pada WPA2-PSK sebanyak 26 pengujian.

Pada gambar 4.38 adalah hasil akhir pengujian pada metode WPA2-PSK



```

Aircrack-ng 1.5.2

[00:12:10] 488133/488132 keys tested (371.17 k/s)
Time left: 0 seconds                               100.00%

KEY NOT FOUND

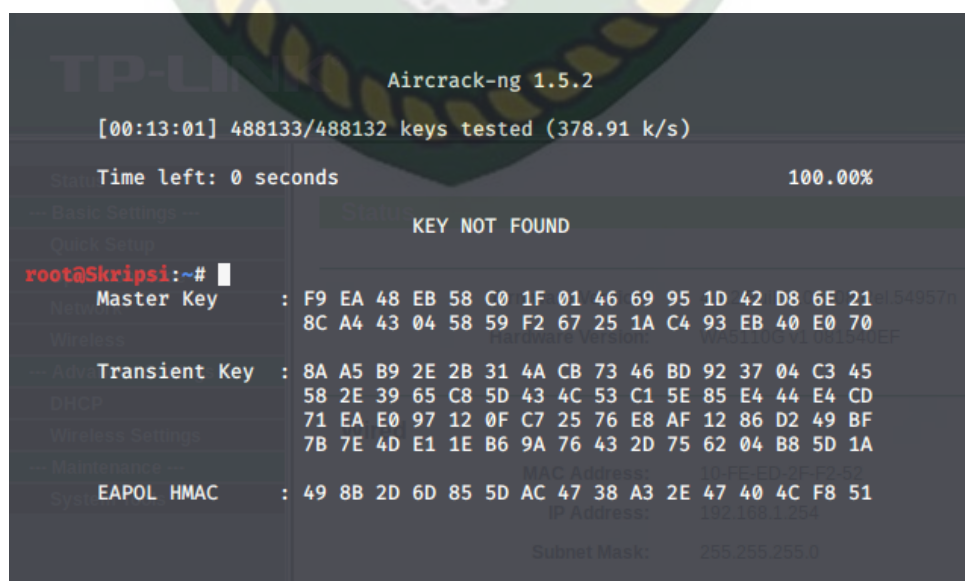
root@Skripsi:~#
Master Key      : 1E 33 AD AA 16 ED 0F 21 0F 13 91 70 DC 70 FD 65
                  6E 8E 67 45 69 43 A9 EE 43 53 97 A2 DC 7A 97 2E

Transient Key   : CA AE 29 4A 7E 4D 23 BC 8B 7C A7 EF E7 8C 9B 58
                  5A 57 2C 4B D3 C1 F3 B3 34 68 6E 3D FE 76 F8 81
                  33 BF 84 54 48 C9 AE 34 3D BE C0 B4 B1 F2 98 1D
                  42 EA 2B 65 AE 47 D5 69 82 28 37 AE 02 8A A9 62

EAPOL HMAC     : DD 93 4C 6E F2 05 87 FB EA A1 7D 64 68 1B 55 7A
  
```

Gambar 4.38 Hasil Akhir Pengujian ke 1

Pada gambar 4.39 adalah hasil akhir pengujian pada metode WPA2-PSK



```

Aircrack-ng 1.5.2

[00:13:01] 488133/488132 keys tested (378.91 k/s)
Time left: 0 seconds                               100.00%

KEY NOT FOUND

root@Skripsi:~#
Master Key      : F9 EA 48 EB 58 C0 1F 01 46 69 95 1D 42 D8 6E 21
                  8C A4 43 04 58 59 F2 67 25 1A C4 93 EB 40 E0 70

Transient Key   : 8A A5 B9 2E 2B 31 4A CB 73 46 BD 92 37 04 C3 45
                  58 2E 39 65 C8 5D 43 4C 53 C1 5E 85 E4 44 E4 CD
                  71 EA E0 97 12 0F C7 25 76 E8 AF 12 86 D2 49 BF
                  7B 7E 4D E1 1E B6 9A 76 43 2D 75 62 04 B8 5D 1A

EAPOL HMAC     : 49 8B 2D 6D 85 5D AC 47 38 A3 2E 47 40 4C F8 51
  
```

Gambar 4.39 Hasil Akhir Pengujian ke 2

Pada gambar 4.40 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2

[00:11:45] 488133/488132 keys tested (378.50 k/s)

Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~#
Master Key      : CE 3F 67 41 D5 6E EC A2 D8 66 40 F0 77 01 11 54
                  94 00 7D 52 7C C5 2C 14 E8 B6 E3 DA CD A6 01 1A

Transient Key   : 63 EF EF EF E6 E5 6E 81 AD 65 D9 D4 23 ED 84 37
                  5D C6 70 DE 8E 4C F2 D0 53 A6 E4 57 4D F6 86 13
                  CD AF E5 D0 27 35 C9 32 80 17 C5 A0 5D 9B E1 D2
                  5F 8D B4 97 CB B3 B1 F3 F4 C8 55 6B AA E0 2A 38

EAPOL HMAC     : 58 01 FC 03 75 4C F5 C7 46 3C 87 33 64 EF 8C A7

```

Gambar 4.40 Hasil Akhir Pengujian ke 3

Pada gambar 4.41 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2

[00:13:18] 488133/488132 keys tested (372.59 k/s)

Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~#
Master Key      : 1E 33 AD AA 16 ED 0F 21 0F 13 91 70 DC 70 FD 65
                  6E 8E 67 45 69 43 A9 EE 43 53 97 A2 DC 7A 97 2E

Transient Key   : F5 0E CE AF 87 F7 EE 48 6A 2E C4 B3 6C F5 06 B6
                  63 5D A1 D9 73 91 E6 B5 4C 9B 1C 29 6C A6 ED 52
                  EF C6 C4 EC D8 B2 EC FE 6D 56 A4 85 08 41 D4 42
                  A7 C0 72 96 E0 45 18 24 D1 E8 A7 00 61 D2 27 8F

EAPOL HMAC     : 80 CC A2 0C 7F BC 86 76 8F A3 6A 9A E5 6B F9 F2

```

Gambar 4.41 Hasil Akhir Pengujian ke 4

Pada gambar 4.42 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2
[00:11:53] 488133/488132 keys tested (382.10 k/s)
Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~# █
Master Key : F9 EA 48 EB 58 C0 1F 01 46 69 95 1D 42 D8 6E 21
             8C A4 43 04 58 59 F2 67 25 1A C4 93 EB 40 E0 70

Transient Key : E5 4B C6 E0 80 AE 39 F1 54 A9 85 00 A8 47 A7 A9
                27 70 48 AF 90 F7 06 2C F9 CB 12 17 DF E6 3A 2C
                0F C9 FA AD 86 32 58 87 33 92 32 BA 08 15 4B BB
                E4 85 BD C6 13 03 86 1E C4 61 69 B3 25 46 29 30

EAPOL HMAC : 13 D7 2D 6D B7 E4 FD 1B 04 83 A7 4A 2A 69 98 90
  
```

Gambar 4.42 Hasil Akhir Pengujian ke 5

Pada gambar 4.43 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2
[00:11:50] 488133/488132 keys tested (374.35 k/s)
Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~# █
Master Key : 99 13 92 4F 6B 6E EB A8 C3 62 7E 0E 08 C1 07 83
             1E 44 91 43 E9 E2 58 84 34 C8 2A 1E 96 54 51 00

Transient Key : 76 1C 9A 08 BC D5 8B E5 E9 E9 13 83 3C 01 9B DE
                C7 B1 2D 2B DD FC 40 CD 72 67 60 C6 58 7B 83 E0
                4B C6 C8 34 08 52 B8 55 01 70 9B BA 59 55 D2 FB
                14 C9 6E B2 26 E1 DC 8F 7C E4 26 8F 79 FA 38 BE

EAPOL HMAC : BC A0 8E F7 13 20 DB D4 50 72 1C E0 EC B2 00 B9
  
```

Gambar 4.43 Hasil Akhir Pengujian ke 6

Pada gambar 4.44 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2
[00:12:16] 488133/488132 keys tested (378.36 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~# █
Master Key      : 92 8C A7 46 8F 53 02 EE E7 DE 3D 16 DA 4C 49 A7
                  65 25 89 91 69 61 83 C9 45 62 91 B5 32 66 84 05
Transient Key   : 90 6F 99 95 AE 9A 33 7F 9D 89 C2 EC 4B F7 F2 9C
                  A1 D6 E2 C0 02 A6 45 3C 10 8E 01 AC 07 A5 A0 15
                  1D 93 73 79 C1 38 E8 CC 7C 07 58 CE 88 70 AB 71
                  F1 FF 91 68 D7 11 06 30 55 57 87 63 21 A4 5D 4D
EAPOL HMAC     : C5 B3 95 DE 79 ED 86 BB 72 0F C4 BC 2B 27 8A ED

```

Gambar 4.44 Hasil Akhir Pengujian ke 7

Pada gambar 4.45 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2
[00:12:33] 488133/488132 keys tested (376.88 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~# █
Master Key      : AF D8 D3 5A 24 9C DC 56 8A 5A 1F 0F A2 CD 41 39
                  02 D8 EF EE 2F D1 7E 31 8A 6E 33 17 FE 46 4C 53
Transient Key   : 77 F2 CC CB 0C 3C 30 E7 AA 34 24 F2 67 E3 1E 15
                  7D 9D 71 A0 F9 39 04 D9 92 3C 65 1F EB 20 48 D4
                  99 76 BF AD 1C A5 8D CD 06 FA 89 C8 1D B2 EA A8
                  CF 56 88 93 E3 BD 45 F4 92 19 10 65 14 15 37 29
EAPOL HMAC     : 57 49 82 29 EA D4 C8 4F FC BE 80 5F 30 D3 31 9D

```

Gambar 4.45 Hasil Akhir Pengujian ke 8

Pada gambar 4.46 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2
[00:12:21] 488133/488132 keys tested (372.99 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~#
Master Key : 6A F8 DC FD 18 16 CB 59 9E 1D A7 98 99 D5 1C 33
             40 31 3F F2 18 F0 F1 25 9C EF 80 D7 64 F5 51 BA
Transient Key : A7 07 61 07 DF D2 FB 81 48 0F CC 46 18 00 BC 4E
                C3 AD EC 1E 0D 82 66 DD D2 AA C4 8D 44 F6 96 E4
                76 FB 35 AD 53 26 7F 9B BC C7 7A FA 89 11 58 81
                24 98 9C 1E 15 2A 94 D7 0A 1C 90 60 AF 9D 30 10
EAPOL HMAC : 48 2F EA DF 71 26 75 A0 11 1B 7F CA 22 38 6F E5

```

Gambar 4.46 Hasil Akhir Pengujian ke 9

Pada gambar 4.47 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2
[00:12:14] 488133/488132 keys tested (375.84 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~#
Master Key : 1E 33 AD AA 16 ED 0F 21 0F 13 91 70 DC 70 FD 65
             6E 8E 67 45 69 43 A9 EE 43 53 97 A2 DC 7A 97 2E
Transient Key : E1 A0 86 B9 8E F3 B4 9D C0 6C 92 D4 E1 BB B0 70
                85 A4 72 9D 81 BA 61 F9 E4 A6 BA E6 43 45 BC C4
                1E F4 F2 C9 72 D8 32 E9 42 B4 56 35 9C E3 85 0D
                75 18 E9 68 A7 B7 5D E2 B0 5D E5 9C C4 D8 93 73
EAPOL HMAC : 2D 79 A9 5C CE E9 15 2A 3A 04 D3 56 64 D7 39 7C

```

Gambar 4.47 Hasil Akhir Pengujian ke 10

Pada gambar 4.48 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2
[00:14:20] 488133/488132 keys tested (376.31 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~#
Master Key      : 2E C7 E7 F3 80 EE 37 0B 56 FE 79 BD 50 D3 DB 02
                  00 DF 93 36 7F D0 0E D7 79 E4 A5 89 09 F7 36 57
Transient Key   : AC 57 59 DE B5 86 32 B5 71 54 0F C7 53 28 2F 70
                  B8 78 34 B5 5E 93 3C 96 14 9C C6 FC A8 85 F2 F3
                  F4 41 71 55 BA 6A A0 C0 D9 ED B7 EB 39 79 E7 AE
                  BC AE 7C 30 69 38 1D 7E 7A E4 25 A5 6F 0E 7C EC
EAPOL HMAC     : 4A 22 12 E4 0A 19 44 7F 24 0C 57 41 28 FE 7A 73

```

Gambar 4.48 Hasil Akhir Pengujian ke 11

Pada gambar 4.49 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2
[00:13:50] 488133/488132 keys tested (376.44 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~#
Master Key      : 55 60 AF F0 37 78 C4 20 8F C9 77 A8 B3 8F AD 68
                  88 26 8B 88 3F 10 BA D1 20 BF 25 B9 2C 5E 39 2B
Transient Key   : F3 57 5C 94 75 86 43 E6 61 97 B4 6B C6 6C F8 D9
                  F8 02 F2 C7 31 85 33 B7 8E AE 25 F2 B4 21 92 10
                  7F ED 62 D5 D9 2B CE 36 B3 AA 44 D1 44 E9 F9 15
                  3B 47 FE 4B 9A 98 47 CD 7A 86 F5 33 8F 55 19 92
EAPOL HMAC     : CD DC 30 FE F7 3C 55 8F A6 0A AD 41 B9 7E E1 36

```

Gambar 4.49 Hasil Akhir Pengujian ke 12

Pada gambar 4.50 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2
[00:12:15] 488133/488132 keys tested (379.78 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~#
Master Key : 55 60 AF F0 37 78 C4 20 8F C9 77 A8 B3 8F AD 68
            88 26 8B 88 3F 10 BA D1 20 BF 25 B9 2C 5E 39 2B
Transient Key : 14 55 3A D0 03 68 90 5F 45 FC 07 E0 CA 40 E7 E0
               9A 50 2B 67 94 DB E1 BB 74 E7 44 8C E9 6E 9C 87
               4E 46 82 E8 C9 5B 30 B5 06 ED E3 B7 78 07 BF 40
               EE EF 5D C1 4D F2 C1 0B 2B 2A 18 51 54 C3 B0 A0
EAPOL HMAC : CC 0C CA E6 F5 59 3A 25 72 AD B8 A7 3F 5D B2 9F

```

Gambar 4.50 Hasil Akhir Pengujian ke 13

Pada gambar 4.51 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2
[00:13:58] 488133/488132 keys tested (372.64 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~#
Master Key : 99 13 92 4F 6B 6E EB A8 C3 62 7E 0E 08 C1 07 83
            1E 44 91 43 E9 E2 58 84 34 C8 2A 1E 96 54 51 00
Transient Key : 9F 49 56 12 CD B1 BA 24 D7 67 9C 74 D5 4D 18 77
               E9 08 40 C2 72 68 FB A1 85 E1 6F 38 5A F3 78 87
               1C 0B D5 DE 6B 8A 32 53 92 6F 07 12 7A 00 A7 56
               11 7C AF 28 A8 07 5E 56 44 75 A1 4E 18 11 64 AC
EAPOL HMAC : 1B 2F AB FB 53 3B BC 5B 74 9C 14 5B A5 F2 7F CE

```

Gambar 4.51 Hasil Akhir Pengujian ke 14

Pada gambar 4.52 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2

[00:12:08] 488133/488132 keys tested (377.67 k/s)

Time left: 0 seconds                                100.00%

KEY NOT FOUND

root@Skripsi:~#
Master Key      : 92 8C A7 46 8F 53 02 EE E7 DE 3D 16 DA 4C 49 A7
                  65 25 89 91 69 61 83 C9 45 62 91 B5 32 66 84 05

Transient Key   : ED 6C FE E1 A5 56 0E 0A E5 BB 67 60 0F B1 0D 99
                  2E AC C2 D4 AC 77 AA D5 30 88 B3 9D 89 34 09 E6
                  5F A7 F0 C5 47 CE 8B 7B 59 95 A2 5B 91 AD 62 58
                  40 11 46 9B 4D 9C 70 DB D7 DD 96 C8 F6 92 46 41

EAPOL HMAC     : 87 8A AB B2 D5 0A F0 EF 0B 66 EC C4 AB 42 15 0E

```

Gambar 4.52 Hasil Akhir Pengujian ke 15

Pada gambar 4.53 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2

[00:22:00] 488133/488132 keys tested (371.09 k/s)

Time left: 0 seconds                                100.00%

KEY NOT FOUND

root@Skripsi:~#
Master Key      : 8A 27 F4 2B F5 1E 2D 06 98 D3 93 74 38 93 60 9D
                  76 2D BF A6 4E C8 BB 96 D3 95 45 E6 D6 1F B5 2E

Transient Key   : 7D 9B B8 B9 AF 45 14 00 9F BC 82 AE 6C 01 E0 D2
                  39 4F 70 09 2F 31 27 40 70 31 04 09 BB AF 6E 53
                  F9 C5 16 5E FF 10 9B F9 4B 79 85 87 08 BB 14 8C
                  03 EC F6 4E 7C 82 07 5C 08 37 A1 AF 5F E9 AE 0C

EAPOL HMAC     : DA 67 A7 C9 AF 77 84 CA F4 AB F5 9B CA 29 8A FF

```

Gambar 4.53 Hasil Akhir Pengujian ke 16

Pada gambar 4.54 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2
[00:17:05] 488133/488132 keys tested (379.92 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~#
Master Key      : 64 FC 86 2E 9C 7F C5 F0 65 25 AA E5 D0 AB 42 53
                  BF 23 66 FE 78 3B 16 10 51 BE 05 DB FD A9 38 2E
Transient Key   : AE 59 92 EF 97 79 1E C7 DE 57 A9 46 F6 54 97 9D
                  E1 D5 13 6A 2C 16 40 89 3E 7B 4A E9 4E D7 0D 64
                  51 CC C5 A7 AA 17 D9 93 70 66 B3 FA 68 B6 1D C7
                  B8 00 41 F0 42 F7 4B C6 C9 5E B3 5C 19 35 34 D5
EAPOL HMAC     : E7 E3 07 26 E8 04 1E 29 C9 18 8F ED A3 95 C8 43

```

Gambar 4.54 Hasil Akhir Pengujian ke 17

Pada gambar 4.55 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2
[00:16:40] 488133/488132 keys tested (381.33 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~#
Master Key      : CE 3F 67 41 D5 6E EC A2 D8 66 40 F0 77 01 11 54
                  94 00 7D 52 7C C5 2C 14 E8 B6 E3 DA CD A6 01 1A
Transient Key   : 4C 19 19 19 99 7E 6A DE FF A3 D5 28 88 24 6F 4F
                  A6 B2 27 58 18 58 6C 86 6A FF 32 DE 79 0B 1B CE
                  2F 28 BD FA 4E 71 AC C7 39 29 5E BD AA 23 16 4A
                  F2 A5 2F 59 C3 EC 2A 6C B6 36 04 A3 71 34 30 DE
EAPOL HMAC     : 8E 02 C6 9A 78 4B 5C 81 DA 35 08 9A C1 76 5A C4

```

Gambar 4.55 Hasil Akhir Pengujian ke 18

Pada gambar 4.56 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2

[00:13:29] 488133/488132 keys tested (381.15 k/s)
Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~#
Master Key : 92 8C A7 46 8F 53 02 EE E7 DE 3D 16 DA 4C 49 A7
             65 25 89 91 69 61 83 C9 45 62 91 B5 32 66 84 05

Transient Key : F3 2E F8 F7 05 9F F6 EA 4A 7C E1 C8 C2 29 C4 1F
                57 19 DB E4 22 9D 4A C3 29 37 DB D0 82 67 A4 74
                F4 E9 F1 72 D7 E3 B5 F6 62 AB 6C 88 2B 50 07 09
                DA 13 E9 82 0A 1B E0 CB A2 7F EC 6D A9 A6 4A EA

EAPOL HMAC : 20 4F 93 43 FB D4 36 9E 2C DB 5A B9 B2 F1 ED B2

```

Gambar 4.56 Hasil Akhir Pengujian ke 19

Pada gambar 4.57 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2

[00:12:42] 488133/488132 keys tested (380.77 k/s)
Time left: 0 seconds 100.00%

KEY NOT FOUND

root@Skripsi:~#
Master Key : 92 8C A7 46 8F 53 02 EE E7 DE 3D 16 DA 4C 49 A7
             65 25 89 91 69 61 83 C9 45 62 91 B5 32 66 84 05

Transient Key : D4 2F CA 1A 4D 04 F7 7B 80 B6 12 CE 87 F5 4A 21
                CF C2 F8 91 85 A6 EE 33 86 7A A5 1E 46 99 25 91
                12 2E B1 94 1E 35 F5 AF 0E BB F8 44 7B 6F 88 3C
                8B C1 1D 13 FC 48 4B 05 A0 FA DE 81 F8 8F 89 33

EAPOL HMAC : 60 64 C1 1A 1C F9 68 1B 47 5C F0 B0 06 41 36 76

```

Gambar 4.57 Hasil Akhir Pengujian ke 20

Pada gambar 4.58 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2
[00:11:55] 488133/488132 keys tested (381.21 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~#
Master Key      : 8A 27 F4 2B F5 1E 2D 06 98 D3 93 74 38 93 60 9D
                  76 2D BF A6 4E C8 BB 96 D3 95 45 E6 D6 1F B5 2E
Transient Key   : B1 59 DA 87 E6 F6 76 0F A5 82 FA E5 6D 86 51 E7
                  A3 D7 A7 FA BD DE B8 AA 89 FC EA 6C D3 DC E8 83
                  74 09 6C 60 9F E7 33 BD E6 7B BB 4C A2 28 D0 8F
                  7F 3A B2 8E 59 69 28 81 0C C1 B2 79 9B 52 22 A8
EAPOL HMAC     : A9 1F A6 C1 58 AC A7 15 89 9E 52 FB 52 CD 59 22

```

Gambar 4.58 Hasil Akhir Pengujian ke 21

Pada gambar 4.59 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2
[00:15:37] 488133/488132 keys tested (378.54 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~#
Master Key      : CE 3F 67 41 D5 6E EC A2 D8 66 40 F0 77 01 11 54
                  94 00 7D 52 7C C5 2C 14 E8 B6 E3 DA CD A6 01 1A
Transient Key   : EB A4 A4 A4 97 33 F9 DB 9E A3 CF 2F 16 25 DC C7
                  BC 14 90 14 1E 79 1A 1C F5 3E F6 3A 7D 0F CC 82
                  AD 55 9B B6 0D A4 1F 47 28 AD A9 7A D1 D6 43 84
                  20 49 4B 60 2E 59 D2 3A 30 0A DC EC 6F D5 DB EE
EAPOL HMAC     : FF B5 96 37 FC 04 87 62 35 A2 D3 6A B2 39 AE 7C

```

Gambar 4.59 Hasil Akhir Pengujian ke 22

Pada gambar 4.60 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2

[00:11:47] 488133/488132 keys tested (381.98 k/s)

Time left: 0 seconds                               100.00%

KEY NOT FOUND

root@Skripsi:~#
Master Key      : 55 60 AF F0 37 78 C4 20 8F C9 77 A8 B3 8F AD 68
                 88 26 8B 88 3F 10 BA D1 20 BF 25 B9 2C 5E 39 2B

Transient Key   : 50 3A 49 91 A0 63 8C B5 B9 9D BD FB 51 D2 71 D1
                 DD 57 1D 66 9A 5C FA 68 EB A2 83 C1 3B B6 12 43
                 6B 8A 72 AF 5E 2E BE EA 3C 5B 1C A9 8E 6A 3F FA
                 D1 81 CB D7 48 A8 E2 B5 96 AE 9B D0 86 6B 15 24

EAPOL HMAC     : F1 6D ED FB D0 A2 AD 20 CA 3F F0 4D DE 50 F2 CE

```

Gambar 4.60 Hasil Akhir Pengujian ke 23

Pada gambar 4.61 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2

[00:11:56] 488133/488132 keys tested (380.71 k/s)

Time left: 0 seconds                               100.00%

KEY NOT FOUND

root@Skripsi:~# x
Master Key      : 64 FC 86 2E 9C 7F C5 F0 65 25 AA E5 D0 AB 42 53
                 BF 23 66 FE 78 3B 16 10 51 BE 05 DB FD A9 38 2E

Transient Key   : BA E2 A7 B5 AE 88 FE 06 1F 89 D3 87 55 8C 93 CE
                 8F E1 F7 30 21 BF 0A 26 48 EF 40 D5 DF A7 16 7C
                 8F EF E4 3B 89 3B EE 03 48 51 73 66 12 95 73 1F
                 6F 75 8C 22 E8 13 63 B3 9D 88 6C E3 63 E5 9D 69

EAPOL HMAC     : C5 68 10 BE 6B B8 A1 51 A1 A0 2C 01 FA D5 79 87

```

Gambar 4.61 Hasil Akhir Pengujian ke 24

Pada gambar 4.62 adalah hasil akhir pengujian pada metode WPA2-PSK

```

Aircrack-ng 1.5.2
[00:11:59] 488133/488132 keys tested (381.08 k/s)
Time left: 0 seconds 100.00%
KEY NOT FOUND
root@Skripsi:~#
Master Key      : 55 60 AF F0 37 78 C4 20 8F C9 77 A8 B3 8F AD 68
                  88 26 8B 88 3F 10 BA D1 20 BF 25 B9 2C 5E 39 2B
Transient Key   : 70 E4 0D B8 66 45 8B 7C 86 98 24 3B A1 AA 66 63
                  C5 9B 38 2F BB EE 97 2B EB 32 A6 9F 55 07 C7 48
                  18 49 45 BA CA 3F 14 6D 65 58 8F 11 B7 04 57 8A
                  31 78 07 E8 2B 6D B3 97 AE 4C 62 38 3F 3E CA AD
EAPOL HMAC     : 4A 6A B4 B6 10 CD 63 F9 91 CE 29 16 43 90 19 F2

```

Gambar 4.62 Hasil Akhir Pengujian ke 25

Pada gambar 4.63 adalah hasil akhir pengujian yang berhasil pada metode WPA2-PSK.

```

Aircrack-ng 1.5.2
[00:00:08] 5671/488132 keys tested (573.50 k/s)
Time left: 14 minutes, 1 second 1.16%
KEY FOUND! [ Uirunggul2020 ]
Master Key      : 2D E0 F1 37 8B 54 DB 59 98 CF A8 87 B3 63 0F 49
                  BB 18 92 AE 2B 67 84 EE 5F 89 74 95 26 52 35 BC
Transient Key   : AC 69 12 55 DD DC A6 11 0A B5 EB FF 3A 7C AF 6F
                  96 47 8A 9D 94 71 99 C6 57 2D CF 0A E4 6D C5 0A
                  DC 16 66 13 75 FB 46 31 3D 8A 56 15 5E F8 A6 F7
                  13 6C 5E C0 E1 CF 33 E8 9A 76 E3 D2 46 C2 81 C7
EAPOL HMAC     : 0A 78 C1 24 A5 C9 FA 45 C4 8D C6 B1 CD AD 8C 01
root@Skripsi:~#

```

Gambar 4.63 Hasil Akhir Pengujian ke 26

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pembahasan yang sudah dipaparkan dalam penelitian ini yang berjudul Perbandingan Algoritma Keamanan Pada Access Point, maka dapat disimpulkan sebagai berikut :

1. Analisa menggunakan metode WEP, harus memiliki pencarian data yang sesuai dari uniknya kata sandi target.
2. Analisa menggunakan metode WPA-PSK, lebih mudah mendapatkan *Handshake* sebab *security* yang masih mempunyai kekurangan dari metode WPA2-PSK
3. Analisa menggunakan metode WPA2-PSK, lebih sulit mendapatkan *Handshake* sebab *security* yang lebih unggul dari metode yang dibahas oleh penulis.

5.2 Saran

Simulasi yang sedang dibangun ini sangat jauh dari kata sempurna, terdapat kekurangan. Untuk itu sangat di perlukan pengembangan lebih lanjut agar simulasi ini lebih sempurna, adapun saran dari simulasi ini agar lebih baik lagi adalah sebagai berikut :

1. Gunakan *wordlist* bahasa Indonesia karena berdasarkan daerah dimana tempat tinggal. Agar lebih mudah mendapatkan kata sandi target

2. Gunakan kombinasi kata sandi angka huruf dan symbol untuk menjaga keamanan dari serangan brute force.



Dokumen ini adalah Arsip Miitik :

Perpustakaan Universitas Islam Riau

DAFTAR PUSTAKA

- Baihaqi, Yeni Yanti dan Zulfan. 2018 . *Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WI-FI*, Serambi Engineering, Vol. 1
- Sari, Maya Desi, Muh.Yamin dan LM. Bahtiar Aksara, 2017, *Analisis Sistem Keamanan Jaringan Wireless (WEP, WPAPSK/WPA2PSK) MAC Address, Menggunakan Metode Penetration Testing*, semanTIK, Vol. 3
- Setiawan, Deris dan Dian Palupi Rini, 2009, *Analisis Keamanan Jaringan Wireless Yang Menggunakan Captive Portal (Studi Kasus : Warnet Fortran)* Seminar Nasional Electrical Informatic and IT'S Educations
- Setyawan, Bangkit Kurnia Ari dan Melwin Syafrizal, 2012, *Analisis Keamanan Jaringan Wireless Yang Menggunakan Captive Portal (Studi Kasus : Warnet Fortran)*, JURNAL DASI, Vol. 13
- Setiawan, Deris dan Dian Palupi Rini, 2009, *Analisis Perbandingan Sistem Keamanan WEP/WPA/RADIUS Pada Jaringan Publik Wireless Hotspot*, Seminar Nasional Electrical Informatic and IT'S Educations
- Ema, Utami, Jazi Eko Istiyanto, Suwanto Raharjo, 2007, *Metodologi Penelitian Pada Ilmu Komputer*, Seminar Nasional Teknologi
- Amri, Syaiful, 2015, *Analisis Jenis-Jenis Sistem Keamanan Jaringan Wireless Hotspot*. Universitas Sumatra Utara
- Supyianto, Aji 2006, *Analisis Kelemahan Keamanan pada Jaringan Wireless*, Jurnal Teknologi Informasi Dinamik, Vol 1
- Zaim, Siti 2015, *Apakah WPA/WPA2 Benar- Benar Aman? Deksripsi Paket Data Terenkripsi Pada WPA/WPA2*, Seminar Nasional
- Herdiana, Yudi 2014, *Kemanan Pada Jaringan Wireless*, Isu Teknologi Mandala, Vol. 7