LAPORAN TUGAS AKHIR

ANALISIS KELEMAHAN PROTOKOL KEAMANAN WEP, WPA1 DAN WPA2 PADA JARINGAN WIRELESS LAN

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana

Strata-1 Teknik Informatika

Oleh:

Nama : Angga Febrian

NIM : 08523128

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

2012

LEMBAR PENGESAHAN PEMBIMBING

ANALISIS KELEMAHAN PROTOKOL KEAMANAN WEP, WPA1 DAN WPA2 PADA JARINGAN WIRELESS LAN

TUGAS AKHIR

Oleh :

Nama : Angga Febrian

NIM : 08523128

Yogyakarta, 11 Desember 2012

Pembimbing

(Ahmad M.Rafie Pratama, S.T., M.I.T.)

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan dibawah ini

Nama : Angga Febrian

NIM : 08523128

Tugas Akhir dengan judul :

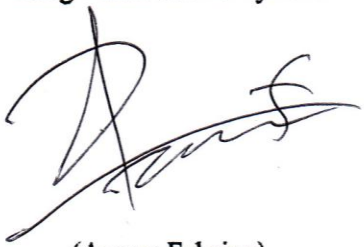
ANALISIS KELEMAHAN PROTOKOL KEAMANAN WEP, WPA1 DAN WPA2 PADA JARINGAN WIRELESS LAN

Dengan ini saya menyatakan dengan sesungguhnya bahwa dalam tugas akhir ini tidak terdapat keseluruhan tulisan atau karya yang saya ambil dengan menyalin serta meniru gagasan atau pendapat atau pemikiran orang lain, yang saya akui seolah-olah sebagai tulisan atau karya saya sendiri.

Apabila saya melakukan hal tersebut, baik sengaja atau tidak, dengan ini saya menyatakan menarik tugas akhir yang saya ajukan sebagai hasil karya saya sendiri. Bila dikemudian hari terbukti bahwa saya melakukan tindakan di atas, gelar dan ijazah yang telah diberikan oleh Universitas Islam Indonesia batal saya terima.

Yogyakarta, 11 Desember 2012

Yang Membuat Pernyataan



(Angga Febrian)

LEMBAR PENGESAHAN DOSEN PENGUJI

ANALISIS KELEMAHAN PROTOKOL KEAMANAN WEP, WPA1 DAN WPA2 PADA JARINGAN WIRELESS LAN

TUGAS AKHIR

Oleh:

Nama : Angga Febrian

NIM : 08523128

Telah Dipertahankan di Depan Sidang Penguji sebagai Salah Satu Syarat

untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika

Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 17 Desember 2012

Tim Penguji

Ahmad M.Rafie Pratama, S.T.,M.I.T.

Ketua

R. Teduh Dirgahayu, S.T., M.Sc., Ph.D.

Anggota I

Hendrik, S.T., M.Eng.

Anggota II

Mengetahui,

Ketua Jurusan Teknik Informatika

Universitas Islam Indonesia

(Yudi Prayudi, S.Si., M.Kom.)

sHALAMAN PERSEMBAHAN

Tugas ahkir ini kupersembahkan untuk

Allah SWT atas karunia dan berkah yang tidak terhingga.

Rasulullah SAW atas ajaran dan bimbingannya yang terus memberikan inspirasi.

Ibunda Sri Mulyani dan Ayahanda Asri Siswanto yang selalu mendukungku dalam keadaan apapun dan tak jemu-jemunya untuk memberi dukungan dan nasihat dalam menjalani kehidupan.

Adik-adikku Ridwan Handoko dan Rifai Iqbal Rifandi agar selalu menjadi yang terbaik bagi keluarga.

Teman-temanku atas bantuan , kritik, dan saran yang sangat berguna dalam membantu penyelesaian tugas ini.

HALAMAN MOTTO

Bacalah dengan (menyebut) nama Tuhanmu yang menciptakan. Dia yang telah menciptakan manusia dari 'alaq. Bacalah, dan tuhanmulah yang Maha Pemurah. Yang mengajar manusia dengan pena, Dia mengajar manusia apa yang tidak diketahuinya. (QS AL 'Alaq (96):1-5)

KATA PENGANTAR

Asslamu'alaikum Wr. Wb.

Puji syukur kehadirat Allah SWT atas rahmat, taufik serta hidayah-Nya laporan tugas akhir dengan judul "Analisis Kelemahan Protokol Keamanan *WEP*, *WPA1* dan *WPA2* pada Jaringan *Wireless LAN*" ini dapat diselesaikan dengan baik.

Tugas akhir ini disusun untuk mengetahui kelemahan protokol keamanan *WEP*, *WPA1* dan *WPA2* terhadap serangan yang berlaku pada jaringan *wireless LAN*. Tugas akhir ini diharapkan dapat memberikan informasi yang bermanfaat bagi pengguna awam maupun network administrator yang menggunakan protokol keamanan *WEP, WPA1* dan *WPA2* untuk menentukan kebijakan keamanan dalam membangun jaringan *wireless LAN*. Ucapan terima kasih sebesar-besarnya kepada semua pihak yang telah membantu dalam penyelesaian tugas akhir ini baik secara langsung maupun tidak langsung. Semoga Allah SWT memberikan limpahan rahmat dan ridho-Nya kepada mereka semua. Ucapan terima kasih dipersembahkan kepada:

1. Allah SWT atas segala rahmat, berkah, dan karunia yang berlimpah tiada pernah habis kepada penulis.
2. Rasulullah SAW atas ajaran, bimbingan, dan warisannya bagi umat manusia.
3. Yang tercinta dan tersayang Ibunda (Sri Mulyani) dan Ayahanda (Asri Siswanto), adikku (Ridwan Handoko) ,dan (Rifai Iqbal Rifandi), semoga Allah SWT memberikan kasih sayang yang berlimpah.
4. Bapak Ahmad M.Rafie Pratama S.T.,MIT selaku dosen pembimbing yang selalu memberikan bimbingan dan saran yang sangat membantu proses pengerjaan tugas akhir ini.
5. Bapak Yudi Prayudi, S.Si., M.Kom selaku Ketua Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia.

6. Seluruh dosen di Jurusan Teknik Informatika UII. Semoga ilmu yang telah diajarkan selama kuliah dapat bermanfaat baik untuk penulis ataupun bagi masyarakat.
7. Untuk Teman Terbaiku Rifki Adisti Irawan yang selalu memotIVasi dan mendukung dalam pengerjaan Tugas Akhir ini.
8. Teman-teman dan saudaraku Angga Pratomo Putro, *ARP*a Adi Tyawan, Danang Bayu Tranggono, Dedeh Mustafa, Gerry Taqwa, Indra Ramdhani, Norman Perdana Putra, Rendy Arinda Praja, Renny Resabty, Riski Apriawan, Rizki Huslapini Kurniawan, Hendra Maulana dan Yuda Ariangga.
9. Teman-teman angkatan 2008 (SNIPER) dan rekan- rekan kelas B di Jurusan Teknik Informatika Universitas Islam Indonesia.
10. Semua pihak yang tidak dapat saya sebutkan satu per satu yang telah membantu baik secara langsung maupun tidak langsung hingga selesainya penyusunan Tugas Akhir ini. Hanya Allah SWT yang dapat membalas amal dan kebaikan kalian semua.

Penulis sangat menyadari keterbatasan pengetahuan dan kemampuan yang dimiliki penulis sehingga jika terdapat banyak kesalahan dalam penulisan laporan tugas akhir ini, penulis mohon maaf sebesar - besarnya serta menerima kritik dan saran demi kebenaran dan kegunaan informasi yang penulis berikan kelak. Semoga laporan tugas akhir ini dapat memberi manfaat baik bagi pribadi penulis, pembaca maupun bagi kita semua. Amin.

Yogyakarta, Desember 2012

Penulis

DAFTAR ISI

LEMBAR PENGESAHAN PEMBIMBING ..... Error! Bookmark not defined.

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR Error! Bookmark not defined.

LEMBAR PENGESAHAN DOSEN PENGUJI .... Error! Bookmark not defined.

HALAMAN PERSEMBAHAN..... v

HALAMAN MOTTO vi

KATA PENGANTAR..... vii

SARI ix

TAKARIR..... x

DAFTAR ISI..... xi

DAFTAR GAMBAR..... xiv

DAFTAR TABEL..... xvi

BAB I..... 1

PENDAHULUAN..... 1

1.1 Latar Belakang..... 1

1.2 Rumusan Masalah..... 2

1.3 Batasan Masalah 2

1.4 Tujuan Penelitian..... 2

1.5 Manfaat Penelitian..... 3

1.6 Metodologi Penelitian 3

1.7 Sistematika Penulisan 3

BAB II 5

LANDASAN TEORI..... 5

2.1 Jaringan Nirkabel (*Wireless*)..... 5

2.1.1 Jaringan Lokal Nirkabel (*Wireless LAN*) 5
2.2 *Wired EquIvalent Privacy* (*WEP*) 5
2.2.1 Otentikasi *Wired EquIvalent Privacy* (*WEP*) 6
2.2.2 Kelemahan *WEP* 8
2.3 *Wi-Fi* Protected Access (*WPA*) 9
2.3.1 *WPA Pre Shared key* 9
2.3.2 Kelemahan *WPA Pre Shared key* 9
2.4 Jenis Jenis Serangan Pada Protokol Keamanan Wireless LAN 10
1. Scanning Wireless Network 10
2. Sniffing Packet 10
3. ARP Request Replay Attack 10
4. Deauthentication Attack 10
5. Cracking WEP 11
6. Dictionary Attack 11
7. *MAC address Spoofing* 11

BAB III 12

METODOLOGI PENELITIAN 12
3.1 Gambaran Umum Sistem 12
3.1.1 Sistem A 12
3.1.2 Sistem B 12
3.1.3 Sistem C 13
3.1.4 Sistem D 13
3.1.5 Topologi Sistem 14
3.2 Kebutuhan Sistem yang digunakan untuk Melakukan Simulasi Pengujian 15
3.2.1 Kebutuhan Perangkat Keras 15
3.2.2 Kebutuhan Perangkat Lunak 16
3.3 Pembangunan Sistem 18
3.3.1 Konfigurasi Umum Sistem A, B, C dan D 18
3.3.2 Konfigurasi Khusus Protokol Keamanan Sistem A 20

3.3.3 Konfigurasi Khusus Protokol Keamanan Sistem B 23
3.3.4 Konfigurasi Khusus Protokol Keamanan Sistem C 26
3.3.5 Konfigurasi Khusus Protokol Keamanan Sistem D 29
3.4 Pengambilan Data 32
3.4.1 Skenario Pengujian..... 32
BAB IV 40
HASIL DAN PEMBAHASAN 40
4.1 Hasil Pengujian..... 40
4.1.1 Sistem A 40
4.1.2 Sistem B 41
4.1.3 Sistem C 43
4.1.4 Sistem D 45
BAB V..... 47
KESIMPULAN DAN SARAN 47
5.1 Kesimpulan 47
5.2 Saran..... 47
DAFTAR PUSTAKA 48

DAFTAR GAMBAR

Gambar 2. 1 Otentikasi pada *Open System Authentication*..... 6

Gambar 2. 2 Otentikasi pada *Shared key Authentication*..... 7

Gambar 3. 1 Topologi Sistem……15

Gambar 3. 2 Konfigurasi Modus Operasi 18

Gambar 3. 3 Konfigurasi LAN..... 19

Gambar 3. 4 Konfigurasi DHCP 19

Gambar 3. 5 Konfigurasi *Wireless* 20

Gambar 3. 6 Konfigurasi Sistem A1 21

Gambar 3. 7 Konfigurasi Sistem A2 21

Gambar 3. 8 Konfigurasi Sistem A3 22

Gambar 3. 9 Konfigurasi Sistem A4 23

Gambar 3. 10 Konfigurasi *Hidden SSID* Sistem B 23

Gambar 3. 11 Konfigurasi *Hidden SSID* Sistem B 24

Gambar 3. 12 Konfigurasi Sistem B1 25

Gambar 3. 13 Konfigurasi Sistem B2 26

Gambar 3. 14 Konfigurasi Sistem C1 27

Gambar 3. 15 Konfigurasi Sistem C2 27

Gambar 3. 16 Konfigurasi Sistem C3 28

Gambar 3. 17 Konfigurasi Sistem C4 28

Gambar 3. 18 Nonaktif SSID Broadcast 29

Gambar 3. 19 Konfigurasi *MAC Filtering* Sistem D 29

Gambar 3. 20 Konfigurasi Sistem D1 30

Gambar 3. 21 Konfigurasi Sistem D2 31

Gambar 3. 22 Konfigurasi Sistem D3 31

Gambar 3. 23 Konfigurasi Sistem D4 32

DAFTAR TABEL

Tabel 3. 1 Uraian Umum Sistem A 12

Tabel 3. 2 Uraian Umum Sistem B 13

Tabel 3. 3 Uraian Umum Sistem C 13

Tabel 3. 4 Uraian Umum Sistem D 14

Tabel 3. 5 Daftar Alamat BSSID dan Pengalamatan IP 15

Tabel 3. 6 Konfigurasi Sistem A1 20

Tabel 3. 7 Konfigurasi Sistem A2 21

Tabel 3. 8 Konfigurasi Sistem A3 22

Tabel 3. 9 Konfigurasi Sistem A4 22

Tabel 3. 10 Konfigurasi Sistem B1 24

Tabel 3. 11 Konfigurasi Sistem B1 25

Tabel 3. 12 Konfigurasi Sistem C1 26

Tabel 3. 13 Konfigurasi Sistem C2 27

Tabel 3. 14 Konfigurasi Sistem C3 28

Tabel 3. 15 Konfigurasi Sistem C4 28

Tabel 3. 16 Konfigurasi Sistem D1 30

Tabel 3. 17 Konfigurasi Sistem D2 30

Tabel 3. 18 Konfigurasi Sistem D3 31

Tabel 3. 19 Konfigurasi Sistem D4 32

Tabel 3. 20 Rangkuman Tahapan Skenario A & B 33

Tabel 3. 21 Rangkuman Tahapan Skenario C & D 37

Tabel 4. 1 Rangkuman Pengujian Skenario A untuk Sistem A 40

Tabel 4. 2 Rangkuman Pengujian Skenario B untuk Sistem B 42

Tabel 4. 3 Rangkuman Pengujian Skenario C untuk Sistem C 44

Tabel 4. 4 Rangkuman Pengujian Skenario D untuk Sistem D 45

SARI

Pada implementasinya, penggunaan protokol keamanan WEP, WPA1 dan WPA 2 sering kurang diperhatikan para praktisi jaringan komputer. Padahal sejak tahun 2001 hingga 2005 isu kelemahan untuk protokol keamanan WEP saja sudah beredar luas, dimana para pakar keamanan seperti Scott Fluhrer, Itsik Mantin, Adi Shamir dan Andreas Klien telah menemukan banyak metode untuk meretas protokol tersebut. Penelitian ini membahas tentang kelemahan yang terdapat pada protokol keamanan WEP, WPA1 dan WPA 2. Pengujian dilakukan dengan cara melakukan serangan yang berlaku pada jaringan wireless LAN pada protokol keamanan WEP, WPA1 dan WPA 2 sesuai dengan kondisi sistem dan skenario pengujian yang telah dibuat penulis. Hasil penelitian menunjukkan bahwa hampir semua protokol keamanan rentan terhadap serangan yang berlaku pada jaringan wireles LAN namun demikian protokol keamanan WPA1 dan WPA2 dengan konfigurasi Hidden SSID dan MAC Filtering jauh lebih unggul terhadap penyusupan dibandingkan protokol keamanan sebelumnya.

Kata Kunci : WEP, WPA1 dan WPA2

TAKARIR

Protocol	Aturan
Device	Alat
Router	Perangkat untuk merutekan data
Client	Pihak yang meminta layanan
Interface	Tampilan dari sebuah program / antarmuka jaringan
Access point	Sebuah perangkat jaringan yang berisi sebuah *transceIVer* dan antena untuk transmisi dan menerima sinyal ke dan dari *clients*
Layer	Lapisan (konsep) dalam jaringan. Berbagai model komunikasi seperti OSI dan TCP/IP terdiri atas beberapa layer yang menyusun protokol tersebut

BAB I
PENDAHULUAN

1.1 Latar Belakang

Sejak munculnya penemuan gelombang radio, teknologi jaringan nirkabel semakin berkembang pesat, seiring ditandainya dengan penemuan modulasi frekuensi oleh Edwin Howard Armstrong yang kemudian berlanjut pada akhir tahun 1970-an, kemudian perusahaan IBM membuktikan kerja kerasnya dengan mengenalkan percobaannya dalam merancang *wireless LAN* pada komputer, meskipun demikian gagal karena tidak memenuhi standart IEEE 802 dengan kecepatan standart LAN yaitu 1 Mbps. Hingga pada tahun 1997 IEEE membuat spesifikasi/standar *wireless LAN* pertama yang diberi kode 802.11.

Dalam perkembangannya orgnasasi IEEE belum mampu memberikan kontribusi ideal untuk perkembangan pasar perangkat keras *wireless LAN*, hingga Cisco mempelopori berdirinya organisasi baru yaitu *Wi-Fi* (*Wireless Fidelity*) dengan tugas memastikan semua peralatan *wireless LAN* dengan label *Wi-Fi* bisa bekerja dengan baik agar konsumen mudah menggunakan produknya. Organisasi *Wi-Fi* membuat peralatan berdasarkan spesifikasi yang telah ditetapkan oleh IEEE meskipun tidak 100% sama, sehingga bisa jadi terdapat fitur yang ditambahkan ke dalam peralatan *wireless* yang tidak ada di dalam standarisasi yang dikeluarkan oleh *IEEE 802.11*.

IEEE dan *Wi-Fi* berusaha saling isi untuk melengkapi kebutuhan standarisasi pada jaringan *wireless LAN*, hal itu terbukti terjadi pada bidang keamanan jaringan *wireless LAN*, dimana IEEE dan *Wi-Fi* merilis berbagai jenis protokol keamanan untuk standar keamanan *wireless LAN*, yang kemudian mengalami penambahan dan model protokol baru yang signifikan. Bermula dari *WEP* (*Wired EquIValent PrIVacy*) yang ditetapkan oleh standar *IEEE 802.11*, menyusul kemudian *WPA1* (*Wi-Fi Protected Access 1*) pada bulan april 2003 dan *WPA2* (*Wi-Fi Protected Access 2*) pada tahun 2004 oleh organisasi *Wi-Fi*. Hingga pada bulan maret 2006 protokol keamanan *WPA2* menjadi sebuah keharusan bagi

peralatan yang bersertifikasi dari aliansi *Wi-Fi* dalam merilis perangkat keras jaringan *wireless*.

Pada implementasinya, penggunaan protokol keamanan *WEP*, *WPA1* dan *WPA2* sering kurang diperhatikan para praktisi jaringan komputer. Padahal sejak tahun 2001 hingga 2005 isu kelemahan untuk protokol keamanan *WEP* saja sudah beredar luas, dimana para pakar keamanan seperti Scott Fluhrer, Itsik Mantin, Adi Shamir dan Andreas Klien telah menemukan banyak metode untuk meretas protokol tersebut. Hingga kini keamanan *WPA1* dan *WPA2* juga memiliki isu penting pada kelemahanya sehingga perlu dilakukan pengujian secara umum untuk mengetahui tingkat keamanan yang terdapat pada *WEP*, *WPA1* dan *WPA2*.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, rumusan masalah pada penelitian ini adalah:

a. Serangan keamanan dan kelemahan apa saja yang berlaku terhadap kerentanan protokol kemanan *WEP*, *WPA1* dan *WPA2* pada jaringan *Wireless LAN*?
b. Dari protokol keamanan *WEP*, *WPA1* dan *WPA2* manakah protokol keamanan yang paling unggul untuk digunakan?

1.3 Batasan Masalah

Batasan masalah yang akan dibahas dalam penelitian ini adalah:

a. Sistem yang akan diujikan tidak menggunakan jaringan internet.
b. Dalam penelitian ini tidak membahas protokol keamanan *WPA1* dan *WPA2* Enterprise dengan *RADIUS Server*.

1.4 Tujuan Penelitian

Memberikan studi referensi kepada akademisi dan praktisi jaringan komputer dalam menentukan kebijakan penggunaan protokol keamanan *WEP*, *WPA1* dan *WPA2* pada jaringan *wireless LAN*.

1.5 Manfaat Penelitian

Dengan dilakukannya penelitian ini, diharapkan dapat memberikan manfaat kepada para akademisi dan praktisi jaringan komputer dalam meningkatkan keamanan pada jaringan *wireless LAN*.

1.6 Metodologi Penelitian

Untuk memenuhi tujuan yang akan dicapai melalui tugas akhir ini, maka ada beberapa metode yang digunakan, yaitu :

1. Studi pustaka untuk mendapatkan informasi dari berbagai buku–buku, makalah, media pembelajaran, dan juga dari sumber internet.
2. Mendesain sistem dan jaringan yang akan diujikan beserta skenario yang akan diujikan selama penelitian.
3. Analisis kebutuhan sistem serta identifikasi mengenai perangkat lunak dan perangkat keras dibutuhkan dalam penelitian ini.
4. Konfigurasi alat dan instalasi sistem berdasarkan skenario yang akan diujikan.
5. Melakukan percobaan terhadap setiap protokol kemanan dengan beberapa skenario yang telah dirancang.
6. Melakukan analisis data dan memberikan kesimpulan terhadap hasil dalam pengujian.

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam pembuatan laporan tugas akhir ini adalah sebagai berikut:

BAB I Pendahuluan

Bab ini membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat dari penelitian, dan metodologi penelitian yang digunakan dalam pelaksanaan tugas akhir mengenai analisis protokol keamanan *WEP, WPA1* dan *WPA2* pada jaringan *wireless LAN*.

BAB II Landasan Teori

Bab ini membahas tentang uraian teori-teori yang berhubungan dengan penelitian tugas akhir yang berisikan penjelasan mengenai jaringan *wireless*, jaringan *wireless LAN*, protokol keamanan *WEP*, *WPA1* dan *WPA2*.

BAB III Metodologi

Bab ini membahas tentang gambaran sistem yang akan diuji, kebutuhan sistem yang akan diuji, pembangunan beserta konfigurasi sistem, dan pengambilan data dengan berbagai jenis skenario serangan yang telah dibuat untuk menguji protokol keamanan *WEP*, *WPA1* dan *WPA2*.

BAB IV Hasil dan Pembahasan

Bab ini membahas tentang hasil pengujian dan analisis yang terjadi terhadap sistem dan skenario yang telah dibuat.

BAB V Penutup

Bab ini berisi kesimpulan dan saran atas hasil seluruh pengujian dalam penelitian.

BAB II
LANDASAN TEORI

2.1 Jaringan Nirkabel (*Wireless*)

Nirkabel (tanpa kabel) atau *wireless* adalah suatu teknik komunikasi atau pertukaran data jarak dekat/jauh tanpa menggunakan kabel. Pada prinsipnya nirkabel dalam melakukan teknik komunikasinya ada yang menggunakan gelombang radio ada pula yang menggunakan sinar.

2.1.1 Jaringan Lokal Nirkabel (*Wireless LAN*)

Jaringan lokal nirkabel (*Wireless LAN*) adalah jaringan area nirkabel (tanpa kabel) yang menggunakan gelombang radio yang dipancarakan sebuah antena dan udara sebagai media transmisinya, gelombang radio ini berfungsi untuk menghubungkan perangkat komputer dengan titik akses tertentu seperti router board ataupun komputer lain. Dengan menggunakan jaringan lokal nirkabel (*Wireless LAN*) pengguna mempunyai mobilitas atau fleksibilitas yang lebih baik dan tidak tergantung pada suatu tempat atau lokasi. (Febrian, 2004 : 456)

2.2 *Wired EquIvalent Privacy* (*WEP*)

Wired EquIvalent Privacy (*WEP*) adalah protokol keamanan yang merupakan bagian dari standar *IEEE 802.11* dan dikembangkan sebagai upaya untuk memberikan pr*IV*asi dalam jaringan nirkabel agar sama dengan pr*IV*asi dalam jaringan kabel. (Hiemstra, 2003 : 84) *WEP* bekerja pada *layer 2 OSI* bertugas untuk mengamankan data dengan mengenkripsi paket yang terdapat pada *MAC* (*Media Access Control*). Setiap *wireless* klien yang tidak mempunyai kunci rahasia dapat melihat lalu lintas data dari jaringan, tetapi semua paket data terenkripsi (Utapea, 2011 : 16).

Standar 802.11 bekerja pada dua lapisan terbawah dari model OSI yaitu lapisan kedua (*data link layer*) dan lapisan pertama (*physical layer*) komunikasi dan transmisi data berlangsung pada lapisan pertama. Lapisan 802.11 *MAC* memberikan berbagai layanan seperti distribusi, integrasi, asosiasi, otentikasi,

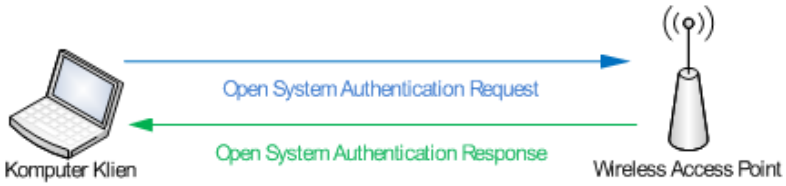
enkripsi dan sebagainya. *WEP* memberikan jaminan keamanan dengan mengenkripsi setiap paket data yang dikirimkan. Algoritma enkripsi yang digunakan *WEP* adalah algoritma enkripsi *RC4*, yaitu algoritma symetric stream cipher dengan panjang kunci 40 bit atau 104 bit. *Initialization Vector* (*IV*) yang digunakan dalam *WEP* adalah sepanjang 24 bit, sehingga sering kali *WEP* dikenal dengan penggunaan kunci 64 bit atau 128 bit yang sebenarnya adalah panjang kunci sebenarnya ditambah dengan panjang *IV*. (Utama, 2011 : 7).

2.2.1 Otentikasi *Wired EquIvalent Privacy* (*WEP*)

Otentikasi adalah tahap awal yang dilakukan untuk melakukan pengenalan mengenai identitas *wireless* client kepada *wireless access point* sebelum dapat mengakses jaringan *wireless LAN*. Tujuan dari otentikasi adalah untuk membuktikan bahwa identitas *wireless* klien yang ingin melakukan proses otentikasi adalah benar. Standart *IEEE 802.11* mendifinisikan dua otentikasi pada protokol keamanan *WEP* diantaranya adalah :

a. *Open System Authentication*

Open System Authentication mengotentikasi semua *wireless* klien yang melakukan permintaan untuk melakukan otentikasi dengan *wireless access point*. Sebenarnya hal ini berarti tidak dilakukan proses otentikasi apapun. (Utama, 2011 : 5). Tahap-tahap dalam proses otentikasi ini dapat dilihat seperti gambar 2.1 berikut ini:



Gambar 2. 1 Otentikasi pada *Open System Authentication*

1. Proses otentikasi diawali dengan pengiriman pesan *Open System Authentication* request dari *wireless* klien menuju *wireless access point* dengan membawa informasi mengenai *MAC address* sebagai alamat asal.

2. Kemudian *wireless access point* akan membalas pesan yang diterima dari *wireless* klien dengan mengirimkan pesan *Open System Authentication* response, yang menandakan berhasil atau tidaknya proses otentikasi tersebut.

b. *Shared key Authentication*

Shared key Authentication melakukan proses otentikasi dengan sebuah kunci rahasia (*shared key*) yang diketahui bersama antara *wireless* klien dengan *wireless access point*. Standar keamanan 802.11 mengasumsikan bahwa kunci rahasia tersebut ditransmisikan ke *wireless* client dengan melalui saluran komunikasi rahasia yang bukan merupakan bagian dari 802.11 (Utama, 2011 : 6). Tahap-tahap dalam proses otentikasi ini dapat dilihat seperti gambar 2.2 berikut ini:

Gambar 2. 2 Otentikasi pada *Shared key Authentication*

1. *Wireless* klien mengirimkan sebuah paket *Shared key Authentication* request kepada *wireless access point*.
2. *Wireless access point* merespon permintaan *wireless* klien dengan mengirimkan sebuah paket *Shared key Authentication* response yang mengandung *challenge text*.
3. *Wireless* klien merespon dengan mengirimkan paket *Shared key Authentication* request yang mengandung *challenge text* yang sudah dienkripsi dengan *Wired EquIvalent Privacy* (*WEP*)
4. *Wireless access point* kemudian mendeskripsi *challenge text* tersebut, dan apabila hasilnya sama dengan *challenge text* yang dibuat wsireless *access point*, maka *access point* akan mengirimkan paket *Shared key Authentication* response yang mengandung informasi bahwa otentikasi berhasil. Sebaliknya,

wireless access point akan mengirimkan *Shared key Authentication* response yang mengandung informasi bahwa otentikasi gagal.

Berbeda dengan *Open System Authentication*, *Shared key Authentication* mengharuskan *wireless* klien untuk mengetahui lebih dahulu kunci rahasia sebelum mengijinkan terkoneksi dengan *wireless access point*. Jadi apabila klien tidak mengetahui kunci tersebut maka klien tidak akan bisa terkoneksi dengan *access point*. Pengecekan *WEP* Key pada proses *Shared key Authentication* dilakukan dengan metode challenge and response sehingga tidak ada proses transfer password kunci *WEP*. (Utama, 2011 : 6)

2.2.2 Kelemahan *WEP*

WEP memiliki berbagai kelemahan, diantaranya adalah :

1. Masalah kunci yang lemah, algoritma *RC4* yang digunakan dapat dipecahkan.
2. *WEP* Menggunakan *Initialization Vector* yang bersifat statis.
3. Masalah *Initialization Vector* (*IV*) *WEP*.
4. Masalah integritas pesan *cyclic redundancy check* (CRC-32).

Serangan-serangan pada kelemahan *WEP* antara lain:

1. Serangan terhadap kelemahan *Initialization Vector* (*IV*), sering disebut *FMS* attack. *FMS* singkatan dari nama ketiga penemu kelemahan *IV* yakni Fluher, Mantin, Shamir. Serangan ini dilakukan dengan cara mengumpulkan *IV* yang lemah sebanyak-banyaknya. Semakin banyak *IV* lemah yang diperoleh, semakin cepat ditemukan kunci yang digunakan. (Prabawati, 2010 : 86).
2. Mendapatkan *IV* yang unik melalui packet data yang diperoleh untuk diolah proses cracking kunci *WEP* dengan lebih cepat. Cara ini disebut chopping attack, pertama kali ditemukan oleh h1kari. Teknik ini hanya membutuhkan *IV* yang unik sehingga mengurangi kebutuhan *IV* yang lemah dalam melakukan *Cracking WEP*. (Prabawati, 2010 : 87).
3. Kedua serangan diatas membutuhkan waktu dan paket yang cukup, untuk mempersingkat waktu, para penyerang biasanya melakukan *traffic injection*. *Traffic injection* yang sering dilakukan adalah dengan cara mengumpulkan

paket *ARP* kemudian mengirimkannya kembali ke *access point*. Hal ini mengakibatkan pengumpulan *IV* lebih mudah dan cepat. (Prabawati, 2010 : 88).

2.3 *Wi-Fi* Protected Access (*WPA*)

Wi-Fi Protected Access (*WPA*) adalah standar yang dikeluarkan oleh aliansi *Wi-Fi* untuk menyediakan keamanan pada standart 802.11 agar menjadi lebih baik, dengan memakai enkripsi yang lebih kuat dalam melakukan otentikasi, dimana didalamnya terdapat enkripsi *Temporal Key Integrity Protocol* (*TKIP*) yang menawarkan distribusi kunci yang dinamis. *RC4* masih digunakan pada protokol keamanan ini. Sembari *WPA* dan *TKIP* dikembangkan agar dapat menjadi lebih aman untuk menggantikan *WEP*, aliansi *Wi-Fi* pun merilis *WPA2* pada tahun 2004 dimana sudah mendukung Advanced Encryption Standard (AES) yang memungkinkan enkripsi yang lebih kuat. (Hiemstra, 2003 : 85)

2.3.1 *WPA Pre Shared key*

WPA personal adalah jenis *WPA* yang digunakan pada skala kecil. *WPA* personal menggunakan metode *Pre Shared key* (*PSK*), yaitu penggunaan kunci rahasia yang dibagi kepada dua belah pihak. Dalam penggunaanya, setiap user harus memasukkan kata kunci untuk mengakses jaringan. Panjang kata kunci dapat bervariasi, yaitu antara 8 sampai 63 karakter. Kata kunci ini sebaiknya tidak disimpan di dalam komputer klien, tetapi harus disimpan pada *access point*. (Utapea, 2011 : 23).

2.3.2 Kelemahan *WPA Pre Shared key*

WPA merupakan teknologi keamanan sementara yang diciptakan untuk menggantikan kunci *WEP*. ada dua jenis yakni *WPA* personal (*WPA-PSK*), dan *WPA*-RADIUS. Saat ini yang sudah dapat diretas adalah *WPA-PSK*, yakni dengan metode *brute force attack* atau *Dictionary Attack* secara offline. Brute force atau *Dictionary Attack* akan menyerang dengan menggunakan mencoba coba banyak kata dari suatu kamus. Serangan ini akan berhasil jika *passphrase* yang

terkandung dalam paket *WPA handshake* menggunakan kata yang terdapat pada kamus penyerang. (Prabawati, 2010 : 87)

2.4 Jenis Jenis Serangan Pada Protokol Keamanan Wireless LAN

1. Scanning Wireless Network

Scanning wireless network adalah sebuah proses untuk melihat, mencari, meneliti serta mendapatkan informasi yang menyeluruh mengenai aktivitas, identitas dan status pada jaringan *wireless* seperti alamat *BSSID*, alamat *ESSID channel*, *frekuensi*, protokol keamanan, enkripsi dan lain lain.

2. Sniffing Packet

Sniffing Packet adalah aktivitas yang dilakukan dengan menyadap paket data yang melintas dalam sebuah jaringan. Paket data ini bisa berisi informasi mengenai apa saja, baik *username* atau hal-hal yang dilakukan melalui pengguna jaringan, tak hanya itu *sniffing packet* dilakukan untuk menganalisis hal yang menyebabkan jaringan macet (Anhar, 2010 : 12).

3. ARP Request Replay Attack

ARP request replay attack adalah jenis serangan pada jaringan *wireless LAN* yang prosesnya dilakukan dengan cara mendengarkan sebuah paket *ARP* kemudian mentransmisikan kembali kembali ke *wireless access point.* Kemudian hal ini menyebabkan *wireless access point* kembali mengulang paket ARP dengan *IV* yang baru dan terjadi terus menerus secara berulang ulang. Kegunaannya adalah untuk melakukan pembanjiran paket data *ARP* untuk menentukan penemuan kunci *WEP* yang yang dibawa oleh *IV*. (D'Otreppe, 2010)

4. Deauthentication Attack

Deauthentication attack adalah jenis serangan yang digolongkan sebagai serangan *denial of service* yang berlaku pada jaringan wireless, serangan ini dilakukan dengan cara mengirimkan paket *disassocate* untuk satu atau lebih pada perangkat keras yang terdapat pada jaringan *wireless* tertentu (D'Otreppe, 2010).

Kegunaan *deauthentication attack* diantaranya adalah:

- Memaksa untuk menampilkan *ESSID* yang tersembunyi pada jaringan Wireless.
- Memaksa klien pada jaringan wireless untuk melakukan *reauthenticate* agar dapat terjadinya pengiriman paket *WPA handshake* pada protokol *WPA1* dan *WPA2*.
- Memaksa terjadinya paket *ARP request*, pasca terputusnya jaringan wireless.

5. Cracking WEP

Cracking WEP adalah jenis serangan peretasan terhadap kunci *WEP* dengan metode *PTW* dan *FMS*, dimana kedua metode ini dieksekusikan pada paket data *Initialization Vector* (*IV*) dengan menggunakan pendekatan statistik dan matematis untuk menemukan kunci *WEP* (D'Otreppe, 2010).

6. Dictionary Attack

Dictionary Attack adalah jenis serangan dengan teknik yang dilakukan untuk mengalahkan mekanisme *cipher* atau otentikasi, dilakukan dengan mencoba menentukan kunci dekripsi atau *passphrase* dengan mencari kemungkinan yang ada. Proses *dictionary attack* dilakukan dengan mencoba secara berturut-turut semua kata dalam daftar yang lengkap disebut kamus. Berbeda dengan *brute force attack*, dimana sebagian besar kunci dicari dengan sistematis, *dictionary attack* mencoba hanya dengan kemungkinan yang paling mungkin berhasil, biasanya berasal dari daftar kata misalnya kamus dan lain-lain (Anonim, 2012).

7. *MAC address Spoofing*

MAC address spoofing adalah teknik serangan yang dilakukan dengan mengubah alamat interface pada *media access control (MAC)* yang telah diberikan oleh pabrikan, dapat dilakukan dengan meniru perangkat lain yang ada dijaringan dengan tujuan untuk melewati *filtering* pada *server* atau *router* (Anonim, 2012).

BAB II
LANDASAN TEORI

2.1 Jaringan Nirkabel (*Wireless*)

Nirkabel (tanpa kabel) atau *wireless* adalah suatu teknik komunikasi atau pertukaran data jarak dekat/jauh tanpa menggunakan kabel. Pada prinsipnya nirkabel dalam melakukan teknik komunikasinya ada yang menggunakan gelombang radio ada pula yang menggunakan sinar.

2.1.1 Jaringan Lokal Nirkabel (*Wireless LAN*)

Jaringan lokal nirkabel (*Wireless LAN*) adalah jaringan area nirkabel (tanpa kabel) yang menggunakan gelombang radio yang dipancarakan sebuah antena dan udara sebagai media transmisinya, gelombang radio ini berfungsi untuk menghubungkan perangkat komputer dengan titik akses tertentu seperti router board ataupun komputer lain. Dengan menggunakan jaringan lokal nirkabel (*Wireless LAN*) pengguna mempunyai mobilitas atau fleksibilitas yang lebih baik dan tidak tergantung pada suatu tempat atau lokasi. (Febrian, 2004 : 456)

2.2 *Wired EquIvalent Privacy* (*WEP*)

Wired EquIvalent Privacy (*WEP*) adalah protokol keamanan yang merupakan bagian dari standar *IEEE 802.11* dan dikembangkan sebagai upaya untuk memberikan pr*IV*asi dalam jaringan nirkabel agar sama dengan pr*IV*asi dalam jaringan kabel. (Hiemstra, 2003 : 84) *WEP* bekerja pada *layer 2 OSI* bertugas untuk mengamankan data dengan mengenkripsi paket yang terdapat pada *MAC* (*Media Access Control*). Setiap *wireless* klien yang tidak mempunyai kunci rahasia dapat melihat lalu lintas data dari jaringan, tetapi semua paket data terenkripsi (Utapea, 2011 : 16).

Standar 802.11 bekerja pada dua lapisan terbawah dari model OSI yaitu lapisan kedua (*data link layer*) dan lapisan pertama (*physical layer*) komunikasi dan transmisi data berlangsung pada lapisan pertama. Lapisan 802.11 *MAC* memberikan berbagai layanan seperti distribusi, integrasi, asosiasi, otentikasi,

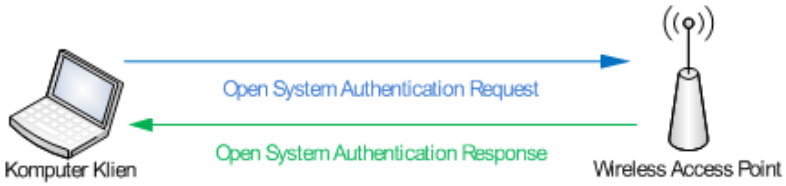
enkripsi dan sebagainya. *WEP* memberikan jaminan keamanan dengan mengenkripsi setiap paket data yang dikirimkan. Algoritma enkripsi yang digunakan *WEP* adalah algoritma enkripsi *RC4*, yaitu algoritma symetric stream cipher dengan panjang kunci 40 bit atau 104 bit. *Initialization Vector* (*IV*) yang digunakan dalam *WEP* adalah sepanjang 24 bit, sehingga sering kali *WEP* dikenal dengan penggunaan kunci 64 bit atau 128 bit yang sebenarnya adalah panjang kunci sebenarnya ditambah dengan panjang *IV*. (Utama, 2011 : 7).

2.2.1 Otentikasi *Wired EquIvalent Privacy* (*WEP*)

Otentikasi adalah tahap awal yang dilakukan untuk melakukan pengenalan mengenai identitas *wireless* client kepada *wireless access point* sebelum dapat mengakses jaringan *wireless LAN*. Tujuan dari otentikasi adalah untuk membuktikan bahwa identitas *wireless* klien yang ingin melakukan proses otentikasi adalah benar. Standart *IEEE 802.11* mendifinisikan dua otentikasi pada protokol keamanan *WEP* diantaranya adalah :

a. *Open System Authentication*

Open System Authentication mengotentikasi semua *wireless* klien yang melakukan permintaan untuk melakukan otentikasi dengan *wireless access point*. Sebenarnya hal ini berarti tidak dilakukan proses otentikasi apapun. (Utama, 2011 : 5). Tahap-tahap dalam proses otentikasi ini dapat dilihat seperti gambar 2.1 berikut ini:



Gambar 2. 1 Otentikasi pada *Open System Authentication*

1. Proses otentikasi diawali dengan pengiriman pesan *Open System Authentication* request dari *wireless* klien menuju *wireless access point* dengan membawa informasi mengenai *MAC address* sebagai alamat asal.

2. Kemudian *wireless access point* akan membalas pesan yang diterima dari *wireless* klien dengan mengirimkan pesan *Open System Authentication* response, yang menandakan berhasil atau tidaknya proses otentikasi tersebut.

b. *Shared key Authentication*

Shared key Authentication melakukan proses otentikasi dengan sebuah kunci rahasia (*shared key*) yang diketahui bersama antara *wireless* klien dengan *wireless access point*. Standar keamanan 802.11 mengasumsikan bahwa kunci rahasia tersebut ditransmisikan ke *wireless* client dengan melalui saluran komunikasi rahasia yang bukan merupakan bagian dari 802.11 (Utama, 2011 : 6). Tahap-tahap dalam proses otentikasi ini dapat dilihat seperti gambar 2.2 berikut ini:

Gambar 2. 2 Otentikasi pada *Shared key Authentication*

1. *Wireless* klien mengirimkan sebuah paket *Shared key Authentication* request kepada *wireless access point*.
2. *Wireless access point* merespon permintaan *wireless* klien dengan mengirimkan sebuah paket *Shared key Authentication* response yang mengandung *challenge text*.
3. *Wireless* klien merespon dengan mengirimkan paket *Shared key Authentication* request yang mengandung *challenge text* yang sudah dienkripsi dengan *Wired EquIvalent Privacy* (*WEP*)
4. *Wireless access point* kemudian mendeskripsi *challenge text* tersebut, dan apabila hasilnya sama dengan *challenge text* yang dibuat wsireless *access point*, maka *access point* akan mengirimkan paket *Shared key Authentication* response yang mengandung informasi bahwa otentikasi berhasil. Sebaliknya,

wireless access point akan mengirimkan *Shared key Authentication* response yang mengandung informasi bahwa otentikasi gagal.

Berbeda dengan *Open System Authentication*, *Shared key Authentication* mengharuskan *wireless* klien untuk mengetahui lebih dahulu kunci rahasia sebelum mengijinkan terkoneksi dengan *wireless access point*. Jadi apabila klien tidak mengetahui kunci tersebut maka klien tidak akan bisa terkoneksi dengan *access point*. Pengecekan *WEP* Key pada proses *Shared key Authentication* dilakukan dengan metode challenge and response sehingga tidak ada proses transfer password kunci *WEP*. (Utama, 2011 : 6)

2.2.2 Kelemahan *WEP*

WEP memiliki berbagai kelemahan, diantaranya adalah :

1. Masalah kunci yang lemah, algoritma *RC4* yang digunakan dapat dipecahkan.
2. *WEP* Menggunakan *Initialization Vector* yang bersifat statis.
3. Masalah *Initialization Vector* (*IV*) *WEP*.
4. Masalah integritas pesan *cyclic redundancy check* (CRC-32).

Serangan-serangan pada kelemahan *WEP* antara lain:

1. Serangan terhadap kelemahan *Initialization Vector* (*IV*), sering disebut *FMS* attack. *FMS* singkatan dari nama ketiga penemu kelemahan *IV* yakni Fluher, Mantin, Shamir. Serangan ini dilakukan dengan cara mengumpulkan *IV* yang lemah sebanyak-banyaknya. Semakin banyak *IV* lemah yang diperoleh, semakin cepat ditemukan kunci yang digunakan. (Prabawati, 2010 : 86).
2. Mendapatkan *IV* yang unik melalui packet data yang diperoleh untuk diolah proses cracking kunci *WEP* dengan lebih cepat. Cara ini disebut chopping attack, pertama kali ditemukan oleh h1kari. Teknik ini hanya membutuhkan *IV* yang unik sehingga mengurangi kebutuhan *IV* yang lemah dalam melakukan *Cracking WEP*. (Prabawati, 2010 : 87).
3. Kedua serangan diatas membutuhkan waktu dan paket yang cukup, untuk mempersingkat waktu, para penyerang biasanya melakukan *traffic injection*. *Traffic injection* yang sering dilakukan adalah dengan cara mengumpulkan

paket *ARP* kemudian mengirimkannya kembali ke *access point*. Hal ini mengakibatkan pengumpulan *IV* lebih mudah dan cepat. (Prabawati, 2010 : 88).

2.3 *Wi-Fi* Protected Access (*WPA*)

Wi-Fi Protected Access (*WPA*) adalah standar yang dikeluarkan oleh aliansi *Wi-Fi* untuk menyediakan keamanan pada standart 802.11 agar menjadi lebih baik, dengan memakai enkripsi yang lebih kuat dalam melakukan otentikasi, dimana didalamnya terdapat enkripsi *Temporal Key Integrity Protocol* (*TKIP*) yang menawarkan distribusi kunci yang dinamis. *RC4* masih digunakan pada protokol keamanan ini. Sembari *WPA* dan *TKIP* dikembangkan agar dapat menjadi lebih aman untuk menggantikan *WEP*, aliansi *Wi-Fi* pun merilis *WPA2* pada tahun 2004 dimana sudah mendukung Advanced Encryption Standard (AES) yang memungkinkan enkripsi yang lebih kuat. (Hiemstra, 2003 : 85)

2.3.1 *WPA Pre Shared key*

WPA personal adalah jenis *WPA* yang digunakan pada skala kecil. *WPA* personal menggunakan metode *Pre Shared key* (*PSK*), yaitu penggunaan kunci rahasia yang dibagi kepada dua belah pihak. Dalam penggunaanya, setiap user harus memasukkan kata kunci untuk mengakses jaringan. Panjang kata kunci dapat bervariasi, yaitu antara 8 sampai 63 karakter. Kata kunci ini sebaiknya tidak disimpan di dalam komputer klien, tetapi harus disimpan pada *access point*. (Utapea, 2011 : 23).

2.3.2 Kelemahan *WPA Pre Shared key*

WPA merupakan teknologi keamanan sementara yang diciptakan untuk menggantikan kunci *WEP*. ada dua jenis yakni *WPA* personal (*WPA-PSK*), dan *WPA*-RADIUS. Saat ini yang sudah dapat diretas adalah *WPA-PSK*, yakni dengan metode *brute force attack* atau *Dictionary Attack* secara offline. Brute force atau *Dictionary Attack* akan menyerang dengan menggunakan mencoba coba banyak kata dari suatu kamus. Serangan ini akan berhasil jika *passphrase* yang

terkandung dalam paket *WPA handshake* menggunakan kata yang terdapat pada kamus penyerang. (Prabawati, 2010 : 87)

2.4 Jenis Jenis Serangan Pada Protokol Keamanan Wireless LAN

1. Scanning Wireless Network

Scanning wireless network adalah sebuah proses untuk melihat, mencari, meneliti serta mendapatkan informasi yang menyeluruh mengenai aktivitas, identitas dan status pada jaringan *wireless* seperti alamat *BSSID*, alamat *ESSID channel*, *frekuensi*, protokol keamanan, enkripsi dan lain lain.

2. Sniffing Packet

Sniffing Packet adalah aktivitas yang dilakukan dengan menyadap paket data yang melintas dalam sebuah jaringan. Paket data ini bisa berisi informasi mengenai apa saja, baik *username* atau hal-hal yang dilakukan melalui pengguna jaringan, tak hanya itu *sniffing packet* dilakukan untuk menganalisis hal yang menyebabkan jaringan macet (Anhar, 2010 : 12).

3. ARP Request Replay Attack

ARP request replay attack adalah jenis serangan pada jaringan *wireless LAN* yang prosesnya dilakukan dengan cara mendengarkan sebuah paket *ARP* kemudian mentransmisikan kembali kembali ke *wireless access point.* Kemudian hal ini menyebabkan *wireless access point* kembali mengulang paket ARP dengan *IV* yang baru dan terjadi terus menerus secara berulang ulang. Kegunaannya adalah untuk melakukan pembanjiran paket data *ARP* untuk menentukan penemuan kunci *WEP* yang yang dibawa oleh *IV*. (D'Otreppe, 2010)

4. Deauthentication Attack

Deauthentication attack adalah jenis serangan yang digolongkan sebagai serangan *denial of service* yang berlaku pada jaringan wireless, serangan ini dilakukan dengan cara mengirimkan paket *disassocate* untuk satu atau lebih pada perangkat keras yang terdapat pada jaringan *wireless* tertentu (D'Otreppe, 2010).

Kegunaan *deauthentication attack* diantaranya adalah:

- Memaksa untuk menampilkan *ESSID* yang tersembunyi pada jaringan Wireless.
- Memaksa klien pada jaringan wireless untuk melakukan *reauthenticate* agar dapat terjadinya pengiriman paket *WPA handshake* pada protokol *WPA1* dan *WPA2*.
- Memaksa terjadinya paket *ARP request*, pasca terputusnya jaringan wireless.

5. Cracking WEP

Cracking WEP adalah jenis serangan peretasan terhadap kunci *WEP* dengan metode *PTW* dan *FMS*, dimana kedua metode ini dieksekusikan pada paket data *Initialization Vector* (*IV*) dengan menggunakan pendekatan statistik dan matematis untuk menemukan kunci *WEP* (D'Otreppe, 2010).

6. Dictionary Attack

Dictionary Attack adalah jenis serangan dengan teknik yang dilakukan untuk mengalahkan mekanisme *cipher* atau otentikasi, dilakukan dengan mencoba menentukan kunci dekripsi atau *passphrase* dengan mencari kemungkinan yang ada. Proses *dictionary attack* dilakukan dengan mencoba secara berturut-turut semua kata dalam daftar yang lengkap disebut kamus. Berbeda dengan *brute force attack*, dimana sebagian besar kunci dicari dengan sistematis, *dictionary attack* mencoba hanya dengan kemungkinan yang paling mungkin berhasil, biasanya berasal dari daftar kata misalnya kamus dan lain-lain (Anonim, 2012).

7. *MAC address Spoofing*

MAC address spoofing adalah teknik serangan yang dilakukan dengan mengubah alamat interface pada *media access control (MAC)* yang telah diberikan oleh pabrikan, dapat dilakukan dengan meniru perangkat lain yang ada dijaringan dengan tujuan untuk melewati *filtering* pada *server* atau *router* (Anonim, 2012).

BAB III
METODOLOGI PENELITIAN

3.1 Gambaran Umum Sistem

Berdasarkan studi literatur yang telah dilakukan oleh penulis terkait masalah dengan protokol keamanan *WEP*, *WPA1* dan *WPA2*, maka dari itu penulis melakukan perancangan sistem yang telah dikelompokan berdasarkan jenis protokol keamanan beserta fiturnya, berikut adalah rancangan sistem dengan penamaan bersifat alphabet yang akan dibangun untuk diujikan.

3.1.1 Sistem A

Sistem A adalah nama label umum dari sub sistem A1, A2, A3 dan A4, di mana pada umumnya sistem ini akan mewakili pengujian untuk protokol keamanan *WEP* berserta fitur-fitur yang ada, berikut ini adalah tabel 3.1 berisi mengenai uraian umum tentang sub sistem yang ada pada sistem A:

Tabel 3. 1 Uraian Umum Sistem A

Nama Sistem	Protokol Keamanan	Opsi Keamanan	Enkripsi	Panjang Kunci	*Hidden SSID*	*MAC Filtering*
Sistem A1	*WEP*	*Open System*	N/A	64 bit	Tidak	Tidak
Sistem A2	*WEP*	*Open System*	N/A	128 bit	Tidak	Tidak
Sistem A3	*WEP*	*Shared key*	N/A	64 bit	Tidak	Tidak
Sistem A4	*WEP*	*Shared key*	N/A	128 bit	Tidak	Tidak

3.1.2 Sistem B

Sistem B adalah nama label umum dari sub sistem B1 dan B2, dimana pada umumnya sistem ini sama dengan sistem A mewakili pengujian untuk protokol keamanan *WEP* berserta fitur fitur yang ada pada sistem ini, namum terdapat tambahan aturan yang diberikan yaitu *Hidden SSID* dan *MAC Filtering*,

berikut ini adalah tabel 3.2 berisi mengenai uraian umum tentang sub sistem yang ada pada sistem B:

Tabel 3. 2 Uraian Umum Sistem B

Nama Sistem	Protokol Keamanan	Opsi Keamanan	Enkripsi	Panjang Kunci	*Hidden SSID*	*MAC Filtering*
Sistem B1	*WEP*	*Open System*	N/A	128 bit	ya	ya
Sistem B2	*WEP*	*Shared key*	N/A	128 bit	ya	ya

3.1.3 Sistem C

Sistem C adalah nama label umum dari sub sistem C1, C2, C3 dan C4, dimana pada umumnya sistem ini akan mewakili pengujian untuk protokol keamanan *WPA1* dan *WPA2* dengan opsi keamanan *shared key* berserta fitur fitur yang ada pada sistem ini, berikut ini adalah tabel 3.3 berisi mengenai uraian umum tentang sub sistem yang ada pada sistem C:

Tabel 3. 3 Uraian Umum Sistem C

Nama Sistem	Protokol Keamanan	Opsi Keamanan	Enkripsi	Panjang Kunci	*Hidden SSID*	*MAC Filtering*
Sistem C1	*WPA1*	*Pre Shared key*	*TKIP*	N/A	Tidak	Tidak
Sistem C2	*WPA1*	*Pre Shared key*	AES	N/A	Tidak	Tidak
Sistem C3	*WPA2*	*Pre Shared key*	*TKIP*	N/A	Tidak	Tidak
Sistem C4	*WPA2*	*Pre Shared key*	AES	N/A	Tidak	Tidak

3.1.4 Sistem D

Sistem D adalah nama label umum dari sub sistem D1, D2, D3 dan D4, dimana pada umumnya sistem ini sama dengan sistem C mewakili pengujian

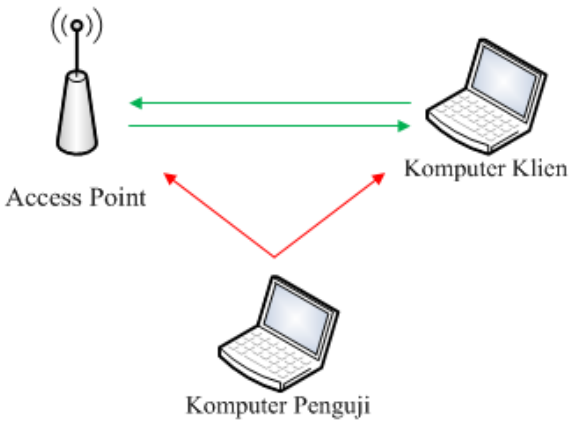
untuk protokol keamanan *WPA1* dan *WPA2* dengan opsi keamanan *shared key* berserta fitur fitur yang ada pada sistem ini namum, namum terdapat tambahan aturan yang diberikan yaitu *Hidden SSID* dan *MAC Filtering*, berikut ini adalah tabel 3.4 berisi mengenai uraian umum tentang sub sistem yang ada pada sistem D:

Tabel 3. 4 Uraian Umum Sistem D

Nama Sistem	Protokol Keamanan	Opsi Keamanan	Enkripsi	Panjang Kunci	*Hidden SSID*	*MAC Filtering*
Sistem D1	*WPA1*	*Pre Shared key*	*TKIP*	N/A	ya	ya
Sistem D2	*WPA1*	*Pre Shared key*	AES	N/A	ya	ya
Sistem D3	*WPA2*	*Pre Shared key*	*TKIP*	N/A	ya	ya
Sistem D4	*WPA2*	*Pre Shared key*	AES	N/A	ya	ya

3.1.5 Topologi Sistem

Dalam pengujian sistem, topologi yang akan dibuat terdiri dari tiga perangkat keras, diantaranya adalah satu buah *wireless access point* router, satu buah komputer laptop yang akan dijadikan sebagai klien yang kemudian akan melakukan otentikasi atau hubungan pada *wireless access point* dan yang terakhir adalah satu buah komputer laptop yang akan mengujinya. Jaringan yang akan digunakan pada pengujian ini adalah jaringan yang bersifat lokal tanpa akses internet. Berikut ini adalah gambar 3.1 yang menggambarkan topologi sistem yang akan diujikan:



Gambar 3. 1 Topologi Sistem

Dengan adanya topologi pada gambar 3.1 diatas, berikut ini adalah tabel 3.5 yang berisi daftar alamat BSSID atau alamat *MAC* dan ketentuan alamat IP pada perangkat yang digunakan untuk pengujian:

Tabel 3. 5 Daftar Alamat BSSID dan Pengalamatan IP

Perangkat	Alamat BSSID	Alamat IP
Wireless access point	00:23:CD:FB:7F:F4	*DHCP Server*
Komputer Klien	00:1E:65:7D:3E:76	*DHCP Server*
Komputer Penguji	00:1E:65:7D:3E:76	*DHCP Server*

3.2 Kebutuhan Sistem yang digunakan untuk Melakukan Simulasi Pengujian

3.2.1 Kebutuhan Perangkat Keras

Berdasarkan gambaran umum sistem yang telah diuraikan, perangkat-perangkat keras yang dibutuhkan untuk mendukung implementasi dari semua fitur-fitur yang ada pada sistem adalah sebagai berikut :

1. *Wireless access point* (TP-LINK : TL-WR543G)
   - Antenna : Omni-Directional
   - Standart : *IEEE 802.11*g dan *IEEE 802.11*b
   - Dimensions : 174 x 111 x 30mm
   - Security : *WEP* (64, 128, 152 bit), *WPA1* & *WPA2*.
   - DHCP : Server, Client, DHCP Client List dan Address Reservation.

2. Komputer Klien
   - *Processor* : Intel Core 2 Duo CPU T5870 2.00GHz
   - Memori : 2048 MB
   - *Harddisk* : Western Digital WDC WD2500BEVS-0 250GB
   - *Wireless Interface* : Intel PRO/*Wireless* 5100 AGN
3. Komputer Penguji
   - *Processor* : Intel Core 2 Duo T5600 1.83GHz
   - Memori : 2048 MB
   - *Harddisk* : Toshiba MK8034GS 80GB
   - *Wireless Interface* : Intel PRO/*Wireless* 3945 ABG

3.2.2 Kebutuhan Perangkat Lunak

1. Windows 7 Ultimate

   Sistem operasi ini digunakan sebagai sistem operasi pada komputer klien.
2. *Linux* Backtrack 5 R2 (rilis 2)

   Sistem operasi ini digunakan sebagai sistem operasi pada komputer penguji.
3. *Aircrack-ng Suite*

   Program bundle terdiri dari berbagai macam program, dimana didalamnya terdapat kumpulan program sebagai berikut :
   - *Airmon-ng*

     Airmon-ng adalah program yang digunakan untuk membuat virtual *wireless* adapter *Interface* serta mengaktifkan dan menonaktifkan modus monitor pada virtual *wireless* adapter *Interface* yang telah dibuat pada sebuah sistem operasi, khususnya pada *linux*.
   - *Airodump-ng*

     Airodump-ng adalah program yang digunakan untuk melakukan scanning pada jaringan *wireless* serta mampu menampilkan informasi terkait atribut pada jaringan *wireless* seperti ESSID (Extended Service Set Identification), BSSID (Basic Service Set Identifier), channel, frequensi, encryption, cipher, *Authentication*, dan lain lain. Selain itu *Airodump-ng* juga mampu melakukan sniffing atau penangkapan paket data pada berbagai jenis paket

data seperti *PCAP (Packet Capture Data*), *IV*s (*Initialization Vector*), dan beberapa Frame pada jenis jenis paket data yang terdapat pada jaringan *wireless*.

- Aireplay-ng

  Aireplay-ng adalah program yang mempunyai fungsi dasar untuk menangkap, menyuntikan serta memutar ulang frame yang ada di udara. Dalam implementasinya aireplay-ng dapat digunakan untuk menggandakan serta membanjiri paket data *IV*s (*Initialization Vector*) dalam mempermudah proses cracking pada *WEP* dengan *Aircrack-ng*. Dalam beberapa teknik aireplay-ng juga dapat melakukan deotentikasi pada protokol *WEP*, *WPA* & *WPA2*, melakukan otentikasi palsu pada protokol tertentu, menangkap paket *WPA handshake* data pada protokol *WPA*, serta dapat pula membuat maupun memanipulasi frame yang diinginkan jika dibantu dengan packetforge-ng, dan masih banyak lagi kegunaan yang terdapat pada aireplay-ng.

- *Aircrack-ng*

  Aircrack-ng adalah program yang digunakan untuk meretas kunci keamanan standar *IEEE 802.11* yaitu *WEP*, *WPA* dan *WPA* 2, hal ini terjadi ketika *Aircrack-ng* mampu mengembalikan kunci *WEP* yang telah dienkripsi pada sebuah paket data yang telah ditangkap dahulu menggunakan *Airodump-ng*. Didalamnya terdapat berbagai*MAC*am metode dasar seperti *PTW*, *FMS* / KoreK, beberapa penggabungan metode brute force dan *Dictionary Attack*.

4. *MAC* Changer

   MAC Changer adalah program yang tergolong sebagai utilitas yang terdapat pada *linux*, digunakan untuk melihat serta memanipulasi alamat *MAC* pada network *Interface*.

5. Nmap (Network Mapper)

   Nmap adalah program yang berfungsi untuk melakukan scanning pada jaringan komputer, dibuat oleh Gordon Lyon atau Fyodor Vaskovich dan memliki halaman website resmi di *insecure.org*. Dalam implementasinya

nmap memiliki lebih dari 15 teknik scanning yang dapat mengindentifikasi host yang aktif, port yang terbuka identifikasi sistem operasi dan fitur scanning lainnya yang dapat diterapkan pada jaringan komputer.

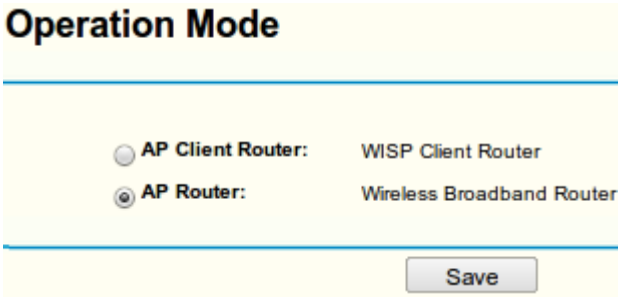
3.3 Pembangunan Sistem

Setelah melakukan persiapan kebutuhan sistem langkah selanjutnya adalah membangun sistem dengan melakukan konfigurasi *wireless access point* berdasarkan sistem yang telah ditentukan pada pembahasan sebelumnya :

3.3.1 Konfigurasi Umum Sistem A, B, C dan D

1. Modus Operasi

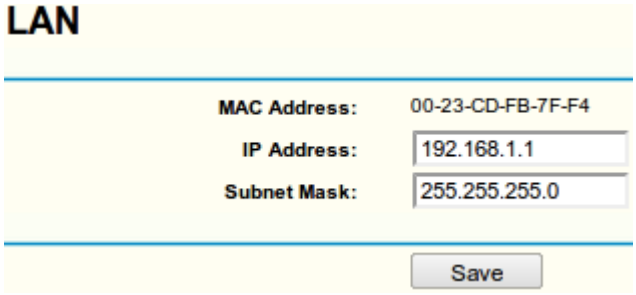
Wireless access point akan dioprasikan dengan modus AP Router dimana *access point* berjalan sebagai router dengan memilih kategori basic settings kemudian menu operation mode lalu memberi pilihan seperti gambar 3.2 dibawah ini:



Gambar 3. 2 Konfigurasi Modus Operasi

2. Status Jaringan

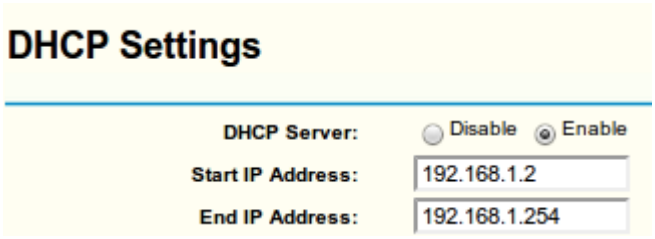
Wireless access point akan dioperasikan dengan status jaringan LAN tanpa menggunakan akses internet dan memiliki alamat ip 192.168.1.1 dengan subnet mask 255.255.255.0, dengan memilih kategori basic settings kemudian menu network lalu sub menu LAN seperti gambar 3.3 dibawah ini:



Gambar 3. 3 Konfigurasi LAN

3. Konfigurasi DHCP

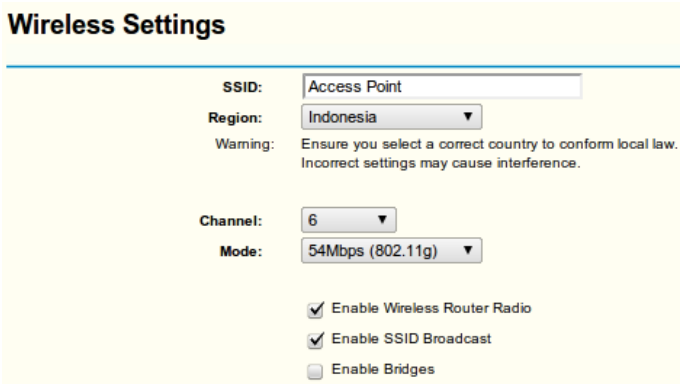
Wireless access point akan dioperasikan sebagai *DHCP Server* dengan ip address yang akan diberikan pada host dimulai dari 192.168.1.2 hingga 192.168.1.254, dengan memilih kategori advanced settings kemudian menu DHCP lalu memberi pilihan seperti gambar 3.4 dibawah ini:



Gambar 3. 4 Konfigurasi DHCP

4. Konfigurasi *Wireless*

Wireless access point akan dioperasikan dengan nama SSID *Access point*, dengan aturan kebijakan penggunaan channel berdasarkan aturan area negara Indonesia, dijalankan pada channel 6 (frekuensi 2,437 GHz) dengan model band 802.11g, dengan memilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings seperti gambar 3.5 dibawah. Untuk konfigurasi SSID broadcast pada sistem B dan D secara khusus akan dioperasikan dengan modus *Hidden SSID*.



Gambar 3. 5 Konfigurasi *Wireless*

3.3.2 Konfigurasi Khusus Protokol Keamanan Sistem A

Secara khusus konfigurasi protokol keamanan pada sistem A akan dikategorikan menjadi 4 jenis berdasarkan sub sistem yang telah dibuat pada pembahasan sebelumnya dan dioprasikan dengan parameter konfigurasi sebagai berikut :

1. Sistem A1

Pada konfigurasi *wireless access point* pilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings, dengan mengaktifkan enable *wireless* security dan memasukan input parameter konfigurasi seperti yang ditampilkan pada tabel 3.6 dan gambar 3.6 dibawah ini:

Tabel 3. 6 Konfigurasi Sistem A1

Parameter Konfigurasi Sistem A1					
Protokol Keamanan	Opsi Keamanan	Format Kunci	Index Kunci	Kunci *WEP*	Panjang Kunci
WEP	*Open System*	ASCII	1	abcde	64 bit

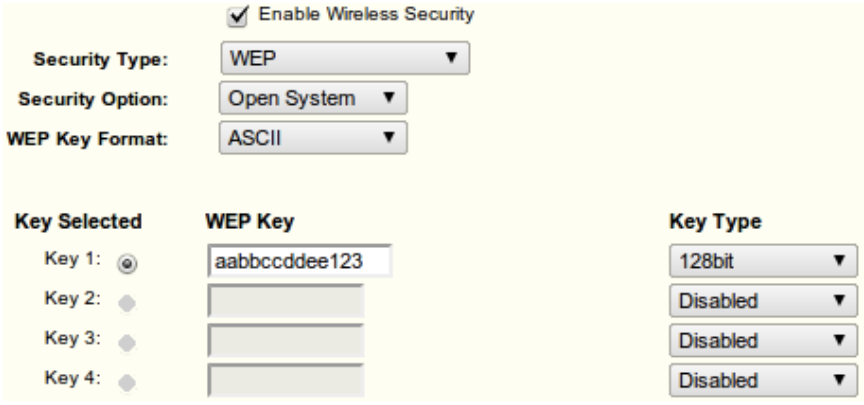
Gambar 3. 6 Konfigurasi Sistem A1

2. Sistem A2

Pada konfigurasi *wireless access point* pilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings, dengan mengaktifkan enable *wireless* security dan memasukan input parameter konfigurasi seperti yang ditampilkan pada tabel 3.7 dan gambar 3.7 dibawah ini:

Tabel 3. 7 Konfigurasi Sistem A2

Parameter Konfigurasi Sistem A2					
Protokol Keamanan	Opsi Keamanan	Format Kunci	Index Kunci	Kunci *WEP*	Panjang Kunci
WEP	*Open System*	ASCII	1	aabbccddee123	128 bit



Gambar 3. 7 Konfigurasi Sistem A2

3. Sistem A3

Pada konfigurasi *wireless access point* pilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings, dengan mengaktifkan enable *wireless* security dan memasukan input parameter konfigurasi seperti yang ditampilkan pada tabel 3.8 dan gambar 3.8 dibawah ini:

Tabel 3. 8 Konfigurasi Sistem A3

Parameter Konfigurasi Sistem A3					
Protokol Keamanan	Opsi Keamanan	Format Kunci	Index Kunci	Kunci *WEP*	Panjang Kunci
WEP	*Shared key*	ASCII	1	abcde	64 bit

Gambar 3. 8 Konfigurasi Sistem A3

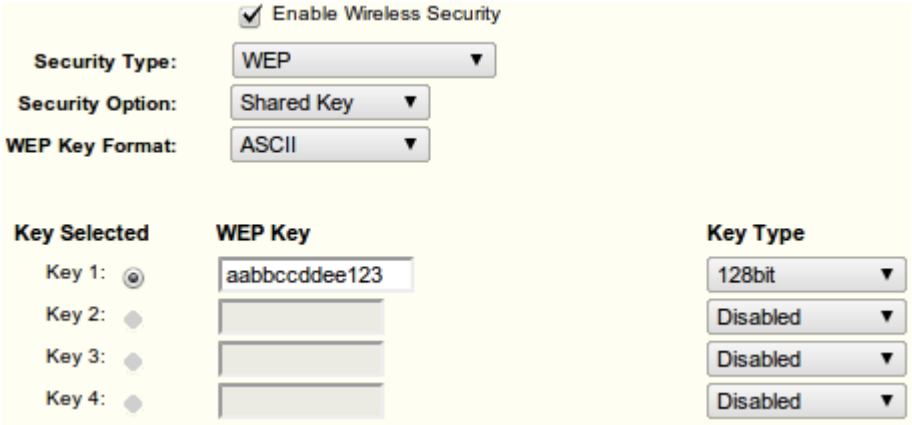
4. Sistem A4

Pada konfigurasi *wireless access point* pilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings, dengan mengaktifkan enable *wireless* security dan memasukan input parameter konfigurasi seperti yang ditampilkan pada tabel 3.9 dan gambar 3.9 dibawah ini:

Tabel 3. 9 Konfigurasi Sistem A4

Parameter Konfigurasi Sistem A4					
Protokol	Opsi	Format	Index	Kunci *WEP*	Panjang

Keamanan	Keamanan	Kunci	Kunci		Kunci
WEP	*Shared key*	ASCII	1	aabbccddee123	128 bit



Gambar 3. 9 Konfigurasi Sistem A4

3.3.3 Konfigurasi Khusus Protokol Keamanan Sistem B

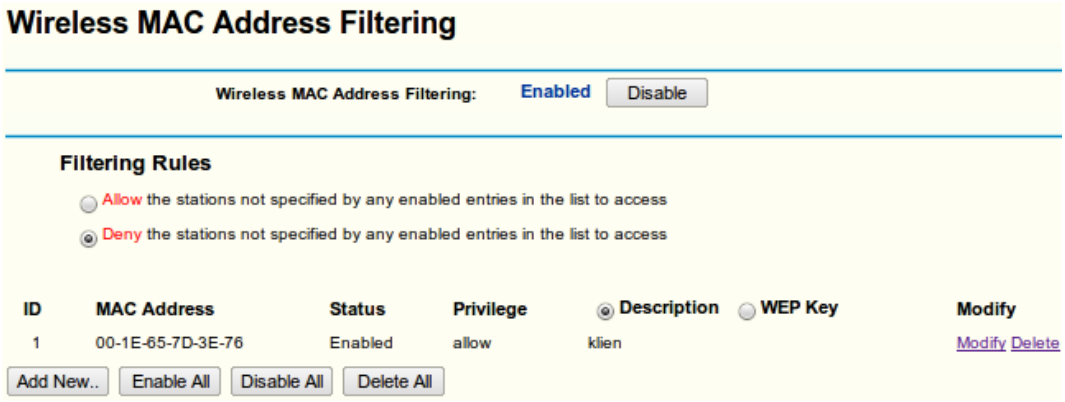
Secara khusus konfigurasi protokol keamanan pada sistem B akan dikategorikan menjadi 2 jenis berdasarkan sub sistem yang telah dibuat pada pembahasan sebelumnya dan dioprasikan dengan parameter konfigurasi sebagai berikut :

Seperti yang telah diterangkan pada pembahasan sebelumnya bahwa untuk sistem B akan dioperasikan dengan modus *Hidden SSID*, dengan memilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings kemudian nonaktifkan enable SSID broadcast seperti gambar 3.10 dibawah ini.

Gambar 3. 10 Konfigurasi *Hidden SSID* Sistem B

Langkah selanjutnya iyalah melakukan konfigurasi *MAC Filtering* dengan dengan memilih kategori basic settings kemudian menu *wireless* lalu sub menu *MAC*

Filtering kemudian aktifkankan service *MAC Filtering* dengan memberikan aturan menolak semua stasion host (klien) kecuali yang tertera aktif pada daftar list yang telah ditentukan pada tabel konfigurasi. Selanjutnya isikan alamat *MAC address* atau bssid komputer klien yaitu 00-1E-65-7D-3E-76, artinya *wireless access point* hanya akan menerima otentikasi komputer dengan alamat *MAC* ini, dapat dilihat pada gambar 3.11 dibawah ini.



Gambar 3. 11 Konfigurasi *Hidden SSID* Sistem B

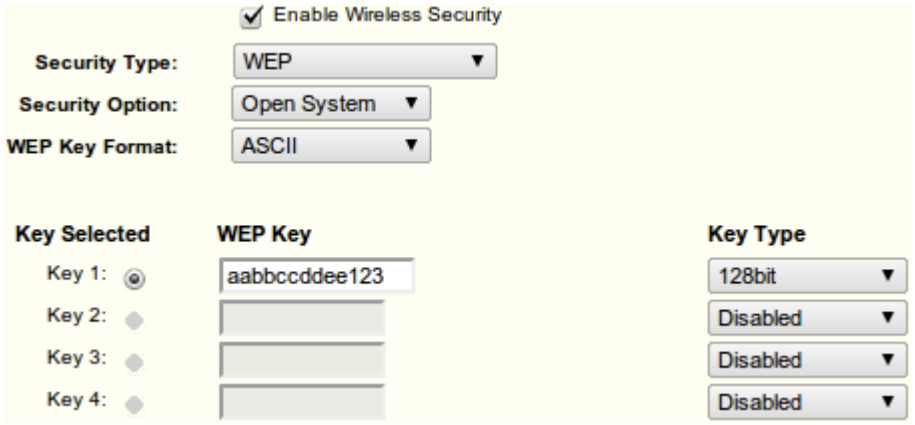
1. Sistem B1

Pada konfigurasi *wireless access point* pilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings, dengan mengaktifkan enable *wireless* security dan memasukan input parameter konfigurasi seperti yang ditampilkan pada tabel 3.10 dan gambar 3.12 dibawah ini:

Tabel 3. 10 Konfigurasi Sistem B1

Parameter Konfigurasi Sistem B1	
Protokol Keamanan	*WEP*
Opsi Keamanan	*Open System*
Format Kunci	ASCII
Index Kunci	1
Kunci *WEP*	aabbccddee123
Panjang Kunci	128 bit
Hidden SSID	ya

MAC Filtering	ya



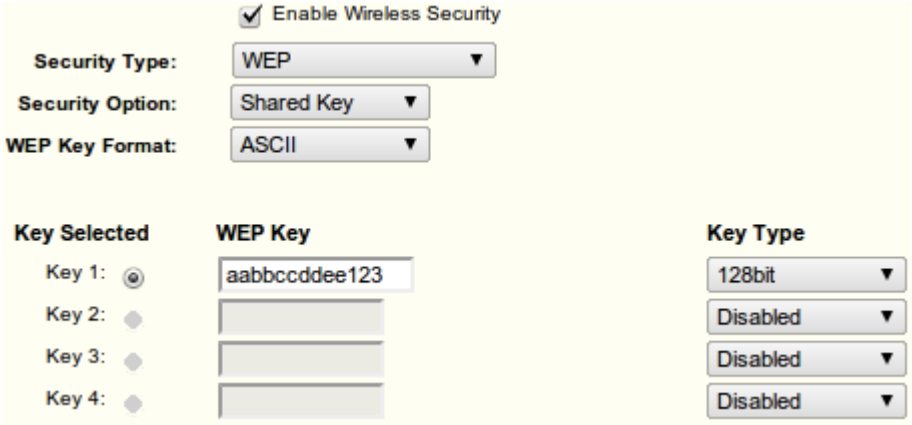
Gambar 3. 12 Konfigurasi Sistem B1

2. Sistem B2

Pada konfigurasi *wireless access point* pilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings, dengan mengaktifkan enable *wireless* security dan memasukan input parameter konfigurasi seperti yang ditampilkan pada tabel 3.11 dan gambar 3.13 dibawah ini:

Tabel 3. 11 Konfigurasi Sistem B1

Parameter Konfigurasi Sistem B2	
Protokol Keamanan	*WEP*
Opsi Keamanan	*Shared key*
Format Kunci	ASCII
Index Kunci	1
Kunci *WEP*	aabbccddee123
Panjang Kunci	128 bit
Hidden SSID	ya
MAC Filtering	ya



Gambar 3. 13 Konfigurasi Sistem B2

3.3.4 Konfigurasi Khusus Protokol Keamanan Sistem C

Secara khusus konfigurasi protokol keamanan pada sistem C akan dikategorikan menjadi 4 jenis berdasarkan sub sistem yang telah dibuat pada pembahasan sebelumnya dan dioprasikan dengan parameter konfigurasi sebagai berikut :

1. Sistem C1

Pada konfigurasi *wireless access point* pilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings, dengan mengaktifkan enable *wireless* security dan memasukan input parameter konfigurasi seperti yang ditampilkan pada tabel 3.12 dan gambar 3.14 dibawah ini:

Tabel 3. 12 Konfigurasi Sistem C1

Parameter Konfigurasi Sistem C1			
Protokol Keamanan	Opsi Keamanan	Enkripsi	*Passphrase*
WPA1	*Pre Shared key*	*TKIP*	abcdefabcdef

Gambar 3. 14 Konfigurasi Sistem C1

2. Sistem C2

Pada konfigurasi *wireless access point* pilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings, dengan mengaktifkan enable *wireless* security dan memasukan input parameter konfigurasi seperti yang ditampilkan pada tabel 3.13 dan gambar 3.15 dibawah ini:

Tabel 3. 13 Konfigurasi Sistem C2

Parameter Konfigurasi Sistem C2			
Protokol Keamanan	Opsi Keamanan	Enkripsi	*Passphrase*
WPA1	*Pre Shared key*	AES	abcdefabcdef

Gambar 3. 15 Konfigurasi Sistem C2

3. Sistem C3

Pada konfigurasi *wireless access point* pilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings, dengan mengaktifkan enable *wireless* security dan memasukan input parameter konfigurasi seperti yang ditampilkan pada tabel 3.14 dan gambar 3.16 dibawah ini:

Tabel 3. 14 Konfigurasi Sistem C3

Parameter Konfigurasi Sistem C3			
Protokol Keamanan	Opsi Keamanan	Enkripsi	*Passphrase*
WPA2	*Pre Shared key*	*TKIP*	abcdefabcdef

Gambar 3. 16 Konfigurasi Sistem C3

4. Sistem C4

Pada konfigurasi *wireless access point* pilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings, dengan mengaktifkan enable *wireless* security dan memasukan input parameter konfigurasi seperti yang ditampilkan pada tabel 3.15 dan gambar 3.17 dibawah ini:

Tabel 3. 15 Konfigurasi Sistem C4

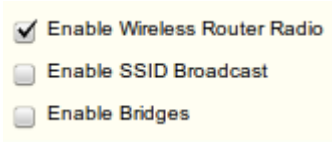
Parameter Konfigurasi Sistem C4			
Protokol Keamanan	Opsi Keamanan	Enkripsi	*Passphrase*
WPA2	*Pre Shared key*	AES	abcdefabcdef

Gambar 3. 17 Konfigurasi Sistem C4

3.3.5 Konfigurasi Khusus Protokol Keamanan Sistem D

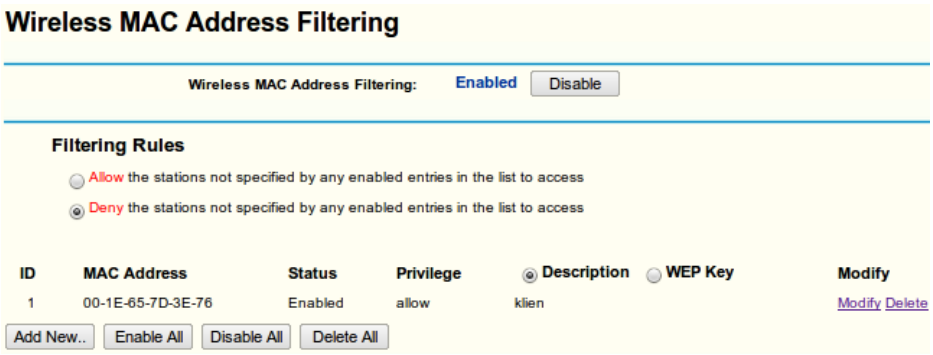
Secara khusus konfigurasi protokol keamanan pada sistem D akan dikategorikan menjadi 4 jenis berdasarkan sub sistem yang telah dibuat pada pembahasan sebelumnya dan dioprasikan dengan parameter konfigurasi sebagai berikut :

Sama seperti B akan dioperasikan dengan modus *Hidden SSID*, dengan memilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings kemudian nonaktifkan enable SSID broadcast seperti gambar 3.18 dibawah ini.



Gambar 3. 18 Nonaktif SSID Broadcast

Kemudian langkah selanjutnya iyalah melakukan konfigurasi *MAC Filtering* dengan dengan memilih kategori basic settings kemudian menu *wireless* lalu sub menu *MAC Filtering* kemudian aktifkankan service *MAC Filtering* dengan memberikan aturan menolak semua stasion host (klien) kecuali yang tertera aktif pada daftar list yang telah ditentukan pada tabel konfigurasi. Selanjutnya isikan alamat *MAC address* atau bssid komputer klien yaitu 00-1E-65-7D-3E-76, artinya *wireless access point* hanya akan menerima otentikasi komputer dengan alamat *MAC* ini seperti gambar 3.19 dibawah ini:



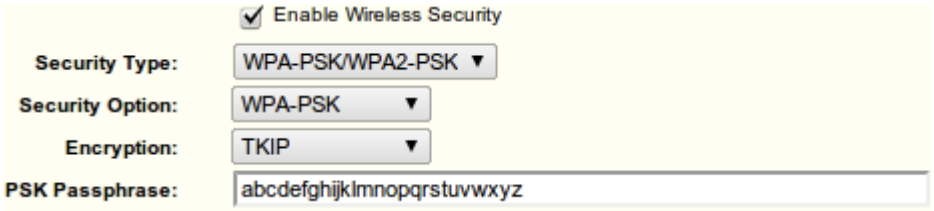
Gambar 3. 19 Konfigurasi *MAC Filtering* Sistem D

1. Sistem D1

Pada konfigurasi *wireless access point* pilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings, dengan mengaktifkan enable *wireless* security dan memasukan input parameter konfigurasi seperti yang ditampilkan pada tabel 3.16 dan gambar 3.20 dibawah ini:

Tabel 3. 16 Konfigurasi Sistem D1

Parameter Konfigurasi Sistem D1					
Protokol Keamanan	Opsi Keamanan	Enkripsi	*Passphrase*	*Hidden SSID*	*MAC Filtering*
WPA1	*Pre Shared key*	*TKIP*	abcdefabcdef	ya	ya



Gambar 3. 20 Konfigurasi Sistem D1

2. Sistem D2

Pada konfigurasi *wireless access point* pilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings, dengan mengaktifkan enable *wireless* security dan memasukan input parameter konfigurasi seperti yang ditampilkan pada tabel 3.17 dan gambar 3.21 dibawah ini:

Tabel 3. 17 Konfigurasi Sistem D2

Parameter Konfigurasi Sistem D2					
Protokol Keamanan	Opsi Keamanan	Enkripsi	*Passphrase*	*Hidden SSID*	*MAC Filtering*
WPA1	*Pre Shared key*	AES	abcdefabcdef	ya	ya

Gambar 3. 21 Konfigurasi Sistem D2

3. Sistem D3

Pada konfigurasi *wireless access point* pilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings, dengan mengaktifkan enable *wireless* security dan memasukan memasukan input parameter konfigurasi seperti yang ditampilkan pada tabel 3.18 dan gambar 3.22 dibawah ini:

Tabel 3. 18 Konfigurasi Sistem D3

Parameter Konfigurasi Sistem D3					
Protokol Keamanan	Opsi Keamanan	Enkripsi	*Passphrase*	*Hidden SSID*	*MAC Filtering*
WPA2	*Pre Shared key*	*TKIP*	abcdefabcdef	ya	ya

Gambar 3. 22 Konfigurasi Sistem D3

4. Sistem D4

Pada konfigurasi *wireless access point* pilih kategori basic settings kemudian menu *wireless* lalu sub menu *wireless* settings, dengan mengaktifkan enable

wireless security dan memasukan memasukan input parameter konfigurasi seperti yang ditampilkan pada tabel 3.19 dan gambar 3.23 dibawah ini:

Tabel 3. 19 Konfigurasi Sistem D4

Parameter Konfigurasi Sistem D4					
Protokol Keamanan	Opsi Keamanan	Enkripsi	*Passphrase*	*Hidden SSID*	*MAC Filtering*
WPA2	*Pre Shared key*	AES	abcdefabcdef	ya	ya

Gambar 3. 23 Konfigurasi Sistem D4

3.4 Pengambilan Data

Pengambilan data pada penelitian ini sebagian besar dilakukan pada sisi komputer penguji dan hanya beberapa data yang diambil dari komputer klien. sebelum melakukan proses pengambilan data, maka perlu dikondisikan sistem yang akan diuji sesuai jenis sistem yang telah dibuat pada pembahasan sebelumnya. Diawali dengan melakukan konfigurasi, setelah selesai baru kemudian komputer klien melakukan otentikasi kepada *wireless access point* setelah itu tahap pengambilan data dilakukan dengan pengujian dari komputer penguji.

3.4.1 Skenario Pengujian

Dalam penelitian ini penguji membuat dan membagi skenario yang akan digunakan untuk melakukan pengujian pada setiap protokol keamanan yang akan diujikan berikut adalah 4 skenario beserta tahapan dan ketentuannya :

1. Skenario A & B

Skenario A adalah skenario pengujian yang umumnya ditujukan untuk menguji sistem A beserta sub sistem A1, A2, A3, dan A4. Skenario pengujian ini terdiri dari 7 tahap, sedangkan skenario B adalah skenario pengujian yang umumnya ditujukan untuk menguji sistem B beserta sub sistem B1 dan B2 yang terdiri dari 8 tahap, dengan 7 tahap yang sama seperti Skenario A namun terdapat 1 tahap khusus yaitu *MAC address* spoofing yang hanya dilakukan pada skenario B. Berikut ini adalah tabel 3.20 rangkuman tahapan A & B dalam skenario dan penjelasan tahapan yang akan dilakukan pada skenario A & B:

Tabel 3. 20 Rangkuman Tahapan Skenario A & B

Skenario A & B	
Jenis Pengujian & Serangan	
Skenario A	Skenario B
Scanning Wireless Network	*Scanning Wireless Network*
Sniffing Packet	*Sniffing Packet*
ARP Request Replay Attack	*ARP Request Replay Attack*
Deauthentication Attack	*Deauthentication Attack*
Cracking WEP	*Cracking WEP*
Authentication	*MAC address* Spoofing
Proof Authentication	*Authentication*
	Proof Authentication
Ditujukan untuk Sistem	Ditujukan untuk Sistem
Sistem A1	Sistem B1
Sistem A2	Sistem B2
Sistem A3	
Sistem A4	

a. *Scanning Wireless Network* (Tahap untuk Skenario A & B)

Dilakukan melalui komputer penguji dengan mengamati dan mengidentifikasi informasi terkait sistem jaringan yang akan diuji menggunakan program *Airodump-ng* dengan menunggu scanning kurang lebih selama 1 menit, kemudian semua data yang diperlukan seperti alamat bssid, channel, protokol keamanan, nama essid dari *wireless access point* dan bssid dari komputer klien akan diambil sebagai data oleh penguji, untuk digunakan pada tahap selanjutnya. Khusus

skenario B untuk pengujian sistem B informasi identitas nama essid dari *wireless access point* yang masih hidden akan didapatkan setelah proses *Deauthentication Attack* dilakukan.

b. *Sniffing Packet* (Tahap untuk Skenario A & B)

Dilakukan melalui komputer penguji dengan menangkap dan merekam semua aktivitas paket data yang sedang bertransmisi antara *wireless access point* dan komputer klien menggunakan program *Airodump-ng* tujuannya adalah untuk mendapatkan paket data yang membawa *IV*s (*Initialization Vector*) sebanyak banyaknya, khusus skenario B untuk pengujian sistem B tahap ini juga digunakan untuk menangkap paket data yang membawa informasi identitas nama essid dari *wireless access point*. Kemudian penguji perlu menunggu tahap ini dan membiarkan program *Airodump-ng* berjalan untuk sementara waktu sampai tahap berikutnya dilakukan yaitu tahap ketiga *ARP Request Replay Attack* dan tahap keempat *Deauthentication Attack* dilakukan, karena kedua tahap tersebut akan mempengaruhi tahap pembajiran paket data yang akan membawa *IV*s (*Initialization Vector*), sehingga proses perekaman paket data oleh *Airodump-ng* akan berhasil.

c. *ARP Request Replay Attack* (Tahap untuk Skenario A & B)

Dilakukan melalui komputer penguji dengan menunggu sebuah paket *ARP* yang akan melakukan transmisi antara *wireless access point* dan komputer klien, jika sebuah paket *ARP* telah terjadi maka kemudian program aireplay-ng akan mentransmisikan paket *ARP* kembali kepada *wireless access point*, hal ini akan menyebabkan *wireless access point* mengulang pengiriman paket *ARP* kembali dengan *IV*s (*Initialization Vector*) yang baru kepada komputer klien kemudian hal ini akan terjadi secara terus menerus sehingga terjadi pembanjiran paket *ARP* dan paket *IV*s (*Initialization Vector*), selama ini pula proses pada tahap *Sniffing Packet* sebelumnya akan merekam semua paket data tersebut sehingga kemudian paket *IV*s (*Initialization Vector*) ini akan digunakan penguji untuk menentukan kunci *WEP* yang ada, namun karena alasana efesiensi waktu untuk mendapatkan sebuah

paket *ARP* maka dari itu penguji perlu memutuskan secara paksa hubungan otentikasi antara *wireless access point* dengan komputer klien yang akan dibahas pada tahap selanjutnya.

d. *Deauthentication Attack* (Tahap untuk Skenario A & B)

Dilakukan melalui komputer penguji dengan cara mengirimkan paket disassocate sebanyak 1 kali menggunakan program aireplay-ng yang ditujukan kepada *wireless access point* dan komputer klien, tujuannya untuk memaksa *wireless access point* dan komputer klien melakukan pemutusan koneksi otentikasi antara keduanya, sehingga *wireless access point* dan komputer klien akan melakukan koneksi kembali dengan melakukan tahap *Authentication* dan re-association, pada tahap inilah kemudian paket *ARP* akan dikirim dari *wireless access point* menuju komputer klien. Khusus skenario B untuk pengujian sistem B informasi identitas nama essid dari *wireless access point* juga akan dikirim dari *wireless access point* menuju komputer klien.

e. *Cracking WEP* (Tahap untuk Skenario A & B)

Dilakukan melalui komputer penguji dengan cara mengeksekusi hasil pembanjiran paket data pada tahap *Sniffing Packet* menggunakan program *Aircrack-ng*, tujuannya untuk melakukan peretasan terhadap kunci *WEP* dengan metode *PTW* dan *FMS*, dimana kedua metode ini menggunakan pendekatan statistik dan matematis yang sudah disediakan dalam algoritma program *Aircrack-ng* dalam melakukan peretasan terhadap kunci *WEP*.

f. *MAC address* Spoofing (Tahap Khusus untuk Skenario B)

Dilakukan melalui komputer penguji dengan mengubah alamat bssid pada komputer penguji menjadi alamat bssid komputer klien menggunakan program *MAC* changger, tujuannya dalah untuk melakukan penyamaran sebagai komputer klien agar dapat melewati *MAC Filtering* pada *wireless access point*.

g. *Authentication* (Tahap untuk Skenario A & B)

Dilakukan melalui komputer penguji dengan melakukan otentikasi pada *wireless access point*, jika proses berhasil maka penguji akan melakukan validasi hubungan antara komputer penguji dengan *wireless access point* dengan melihat status hubungan koneksi dan melihat status jaringan berdasarkan alamat ip address yang sudah didapat dari servis DHCP.

h. *Proof Authentication* (Tahap untuk Skenario A & B)

Dilakukan melalui komputer penguji dengan melakukan scanning jaringan LAN menggunakan program nmap, jika hasil scanning telah berhasil didapat maka penguji dapat mengetahui alamat ip address dan alamat bssid dari *wireless access point*, yang mana untuk alamat bssid penguji dapat membandingkan apakah alamat bssid tersebut sama dengan hasil scanning sebelumnya, jika sama maka terbukti bahwa penguji berhasil masuk kedalam jaringan yang menggunakan protokol keamanan *WEP*.

2. Skenario C & D

Skenario C adalah skenario pengujian yang umumnya ditujukan untuk menguji sistem C beserta sub sistem C1, C2, C3 dan C4. Skenario pengujian ini terdiri dari 6 tahap, sedangkan skenario D adalah skenario pengujian yang umumnya ditujukan untuk menguji sistem D beserta sub sistem D1, D2, D3 dan D4 yang terdiri dari 7 tahap yang sama seperti Skenario C namun terdapat 1 tahap khusus yaitu *MAC address* spoofing yang hanya dilakukan pada skenario D. Berikut ini adalah tabel 3.21 rangkuman tahapan C & D dalam skenario dan penjelasan tahapan yang akan dilakukan pada skenario C & D:

Tabel 3. 21 Rangkuman Tahapan Skenario C & D

Skenario C & D	
Jenis Pengujian & Serangan	
Skenario C	Skenario D
Scanning Wireless Network	*Scanning Wireless Network*
Sniffing Packet	*Sniffing Packet*
Deauthentication Attack	*Deauthentication Attack*
Dictionary Attack	*Dictionary Attack*
Authentication	*MAC address* Spoofing
Proof Authentication	*Authentication*
	Proof Authentication
Ditujukan untuk Sistem	Ditujukan untuk Sistem
Sistem C1	Sistem D1
Sistem C2	Sistem D2
Sistem C3	Sistem D3
Sistem C4	Sistem D4

a. *Scanning Wireless Network* (Tahap untuk Skenario C & D)

Dilakukan melalui komputer penguji dengan mengamati dan mengidentifikasi informasi terkait sistem jaringan yang akan diuji menggunakan program *Airodump-ng* dengan menunggu scanning kurang lebih selama 1 menit, kemudian semua data yang diperlukan seperti alamat bssid, channel, protokol keamanan, nama essid dari *wireless access point* dan bssid dari komputer klien akan diambil sebagai data oleh penguji, untuk digunakan pada tahap selanjutnya. Khusus skenario D untuk pengujian sistem D informasi identitas nama essid dari *wireless access point* yang masih hidden akan didapatkan setelah proses *Deauthentication Attack* dilakukan.

b. *Sniffing Packet* (Tahap untuk Skenario C & D)

Dilakukan melalui komputer penguji dengan menangkap dan merekam semua aktivitas paket data yang sedang bertransmisi antara *wireless access point* dan komputer klien menggunakan program *Airodump-ng* tujuannya adalah untuk mendapatkan paket data yang membawa *WPA handshake*, khusus skenario B untuk pengujian sistem B tahap ini juga digunakan untuk menangkap paket data

yang membawa informasi identitas nama essid dari *wireless access point*. Kemudian penguji perlu menunggu tahap ini dengan membiarkan program *Airodump-ng* berjalan untuk sementara waktu sampai *WPA handshake* dan informasi nama essid dari *wireless access point* didapatkan, dimana proses ini bergantung pada tahap berikutnya yaitu *Deauthentication Attack*.

c. *Deauthentication Attack* (Tahap untuk Skenario C & D)

Dilakukan melalui komputer penguji dengan cara mengirimkan paket disassocate sebanyak 3 kali menggunakan program aireplay-ng yang ditujukan kepada *wireless access point* dan komputer klien, tujuannya untuk memaksa *wireless access point* dan komputer klien melakukan pemutusan koneksi otentikasi antara keduanya, sehingga *wireless access point* dan komputer klien akan melakukan koneksi kembali dengan melakukan tahap *Authentication* dan re-association, pada tahap inilah kemudian paket *WPA handshake* akan dikirim dari *wireless access point* menuju komputer klien. Khusus skenario D untuk pengujian sistem D informasi identitas nama essid dari *wireless access point* juga akan dikirim dari *wireless access point* menuju komputer klien. Jika proses ini berhasil maka hasilnya akan didapat paket *WPA handshake*, khusus skenario D untuk pengujian sistem D juga akan didapat informasi identitas nama essid dari *wireless access point* yang kemudian akan ditangkap oleh tahap *Sniffing Packet* sebelumnya.

d. *Dictionary Attack* (Tahap untuk Skenario C & D)

Dilakukan melalui komputer penguji dengan cara mencoba secara berturut semua kata, angka atau simbol yang terdapat dalam daftar yang lengkap yang disebut kamus dengan format text, dimana serangan ini akan diimplementasikan dengan program *Aircrack-ng* yang ditujukan kepada hasil penangkapan data *WPA handshake* pada tahap *Sniffing Packet* sebelumnya.

e. *MAC address* Spoofing (Tahap Khusus untuk Skenario D)

Dilakukan melalui komputer penguji dengan mengubah alamat bssid pada komputer penguji menjadi alamat bssid komputer klien menggunakan program

MAC changger, tujuannya dalah untuk melakukan penyamaran sebagai komputer klien agar dapat melewati *MAC Filtering* pada *wireless access point*.

f. *Authentication* (Tahap untuk Skenario C & D)

Dilakukan melalui komputer penguji dengan melakukan otentikasi pada *wireless access point*, jika proses berhasil maka penguji akan melakukan validasi hubungan antara komputer penguji dengan *wireless access point* dengan melihat status hubungan koneksi dan melihat status jaringan berdasarkan alamat ip address yang sudah didapat dari servis DHCP.

g. *Proof Authentication* (Tahap untuk Skenario C & D)

Dilakukan melalui komputer penguji dengan melakukan scanning jaringan LAN menggunakan program nmap, jika hasil scanning telah berhasil didapat maka penguji dapat mengetahui alamat ip address dan alamat bssid dari *wireless access point*, yang mana untuk alamat bssid penguji dapat membandingkan apakah alamat bssid tersebut sama dengan hasil scanning sebelumnya, jika sama maka terbukti bahwa penguji berhasil masuk kedalam jaringan yang menggunakan protokol keamanan *WPA1* ataupun *WPA2*.

BAB IV
HASIL DAN PEMBAHASAN

Bab ini peneliti menampilkan hasil pengujian sistem yang telah dilakukan. Agar lebih mudah dipahami, bab ini dibagi menjadi beberapa subbab sesuai dengan sistem, skenario dan analisis tentang hasil pengujian.

4.1 Hasil Pengujian

4.1.1 Sistem A

Hasil pengujian pada skenario A yang ditujukan untuk sistem A dengan sub sistem A1, A2, A3 dan A4 menunjukan bahwa semua aktivitas dan serangan pada jaringan *wireless LAN* berhasil dilakukan pada protokol keamanan *WEP*. Berikut ini adalah tabel 4.1 berisi tentang rangkuman hasil pengujian skenario A untuk sistem A:

Tabel 4. 1 Rangkuman Pengujian Skenario A untuk Sistem A

Nama Sistem	Protokol Keamanan	Opsi Keamanan	Enkripsi	Panjang Kunci	*Hidden SSID*	*MAC Filtering*
Sistem A1	*WEP*	*Open System*	N/A	64 bit	Tidak	Tidak
Sistem A2	*WEP*	*Open System*	N/A	128 bit	Tidak	Tidak
Sistem A3	*WEP*	*Shared key*	N/A	64 bit	Tidak	Tidak
Sistem A4	*WEP*	*Shared key*	N/A	128 bit	Tidak	Tidak

Berdasarkan sistem A1, A2, A3, dan A4 diatas berikut dibawah ini adalah hasil dan status pengujiannya :

	Skenario A	Status Pengujian
Jenis Pengujian & Serangan	*Scanning Wireless Network*	Berhasil
	Sniffing Packet	Berhasil
	ARP Request Replay Attack	Berhasil
	Deauthentication Attack	Berhasil
	Cracking WEP	Berhasil
	Authentication	Berhasil
	Proof Authentication	Berhasil

Berdasarkan tabel 4.1 diatas rangkuman hasil semua sistem pengujian dapat diketahui bahwa:

- Dengan berhasilnya pengujian *scanning wireless network* maka dari itu dapat dibuktikan bahwa protokol keamanan *WEP* rentan terhadap pencurian informasi terkait dengan identitas sistem dan komponen pada jaringan *wireless LAN*.
- Dengan berhasilnya pengujian *sniffing packet* maka dari itu dapat dibuktikan bahwa protokol keamanan *WEP* rentan terhadap pencurian dan pengambilan paket data yang sedang melakukan transmisi pada jaringan *wireless LAN*.
- Dengan berhasilnya pengujian *ARP request replay attack* maka dari itu dapat dibuktikan bahwa protokol keamanan *WEP* rentan terhadap serangan pembanjiran paket data yang bersumber dari paket *ARP* pada jaringan *wireless LAN*.
- Dengan berhasilnya pengujian *deauthentication attack* maka dari itu dapat dibuktikan bahwa protokol keamanan *WEP* rentan terhadap serangan *denial of service* atau pemutusan koneksi secara paksa pada jaringan wireless LAN.
- Dengan berhasilnya pengujian *cracking WEP* maka dari itu dapat dibuktikan bahwa paket data hasil dari *sniffing packet* pada protokol keamanan *WEP* dapat diretas dengan bantuan aplikasi yang menggunakan metode *PTW* dan *FMS* untuk meretas kunci *WEP*.

4.1.2 Sistem B

Hasil pengujian pada skenario B yang ditujukan untuk sistem B dengan sub sistem B1 dan B2 menunjukan bahwa semua aktivitas dan serangan pada jaringan *wireless LAN* berhasil dilakukan pada protokol keamanan *WEP* dengan tambahan opsi keamanan *hidden SSID* dan *MAC filtering*. Berikut ini adalah tabel 4.2 berisi tentang rangkuman hasil pengujian skenario B untuk sistem B:

Tabel 4. 2 Rangkuman Pengujian Skenario B untuk Sistem B

Nama Sistem	Protokol Keamanan	Opsi Keamanan	Enkripsi	Panjang Kunci	*Hidden SSID*	*MAC Filtering*
Sistem B1	*WEP*	*Open System*	N/A	128 bit	ya	ya
Sistem B2	*WEP*	*Shared key*	N/A	128 bit	ya	ya

Berdasarkan sistem B1 dan B2 diatas berikut dibawah ini adalah hasil dan status pengujiannya:		
Jenis Pengujian & Serangan	Skenario B	Status Pengujian
	Scanning Wireless Network	Berhasil
	Sniffing Packet	Berhasil
	ARP Request Replay Attack	Berhasil
	Deauthentication Attack	Berhasil
	Cracking WEP	Berhasil
	MAC address Spoofing	Berhasil
	Authentication	Berhasil
	Proof Authentication	Berhasil

Berdasarkan tabel 4.2 diatas rangkuman hasil semua sistem pengujian dapat diketahui bahwa:

- Dengan berhasilnya pengujian *scanning wireless network* maka dari itu dapat dibuktikan bahwa protokol keamanan *WEP* dengan tambahan opsi keamanan *hidden SSID* dan *MAC filtering* rentan terhadap pencurian informasi terkait dengan identitas sistem dan komponen pada jaringan *wireless LAN*.
- Dengan berhasilnya pengujian *sniffing packet* maka dari itu dapat dibuktikan bahwa protokol keamanan *WEP* dengan tambahan opsi keamanan *hidden SSID* dan *MAC filtering* rentan terhadap pencurian dan pengambilan paket data yang sedang melakukan transmisi pada jaringan *wireless LAN*.
- Dengan berhasilnya pengujian *ARP request replay attack* maka dari itu dapat dibuktikan bahwa protokol keamanan *WEP* dengan tambahan opsi keamanan *hidden SSID* dan *MAC filtering* rentan terhadap serangan pembanjiran paket data yang bersumber dari paket *ARP* pada jaringan *wireless LAN*.
- Dengan berhasilnya pengujian *deauthentication attack* maka dari itu dapat dibuktikan bahwa protokol keamanan *WEP* dengan tambahan opsi keamanan

hidden SSID dan *MAC filtering* rentan terhadap serangan *denial of service* atau pemutusan koneksi secara paksa pada jaringan wireless LAN.

- Dengan berhasilnya pengujian *cracking WEP* maka dari itu dapat dibuktikan bahwa pada protokol keamanan *WEP* dengan tambahan opsi keamanan *hidden SSID* dan *MAC filtering*, paket data hasil dari *sniffing packet* dapat diretas dengan bantuan aplikasi yang menggunakan metode *PTW* dan *FMS* untuk meretas kunci *WEP*.
- Dengan berhasilnya pengujian *MAC address* spoofing maka dari itu dapat dibuktikan bahwa protokol keamanan *WEP* dengan tambahan opsi keamanan *hidden SSID* dan *MAC filtering* rentan terhadap penyusupan dan penyamaran MAC address dari sisi klien.

4.1.3 Sistem C

Hasil pengujian pada skenario C yang ditujukan untuk sistem C dengan sub sistem C1, C2, C3 dan C4 menunjukan bahwa semua aktivitas dan serangan pada jaringan *wireless LAN* berhasil dilakukan pada protokol keamanan *WPA1* dan *WPA2*. Berikut ini adalah tabel 4.3 berisi tentang rangkuman hasil pengujian skenario C untuk sistem C:

Tabel 4. 3 Rangkuman Pengujian Skenario C untuk Sistem C

Nama Sistem	Protokol Keamanan	Opsi Keamanan	Enkripsi	Panjang Kunci	*Hidden SSID*	*MAC Filtering*
Sistem C1	*WPA1*	*Pre Shared key*	*TKIP*	N/A	Tidak	Tidak
Sistem C2	*WPA1*	*Pre Shared key*	AES	N/A	Tidak	Tidak
Sistem C3	*WPA2*	*Pre Shared key*	*TKIP*	N/A	Tidak	Tidak
Sistem C4	*WPA2*	*Pre Shared key*	AES	N/A	Tidak	Tidak

Berdasarkan sistem C1, C2, C3, dan C4 diatas berikut dibawah ini adalah hasil dan status pengujiannya :		
Jenis Pengujian & Serangan	Skenario C	Status Pengujian
	Scanning Wireless Network	Berhasil
	Sniffing Packet	Berhasil
	Deauthentication Attack	Berhasil
	Dictionary Attack	Berhasil
	Authentication	Berhasil
	Proof Authentication	Berhasil

Berdasarkan tabel 4.3 diatas rangkuman hasil semua sistem pengujian dapat diketahui bahwa:

- Dengan berhasilnya pengujian *scanning wireless network* maka dari itu dapat dibuktikan bahwa protokol keamanan *WPA1* dan *WPA2* rentan terhadap pencurian informasi terkait dengan identitas sistem dan komponen pada jaringan *wireless LAN*.
- Dengan berhasilnya pengujian *sniffing packet* maka dari itu dapat dibuktikan bahwa protokol keamanan *WPA1* dan *WPA2* rentan terhadap pencurian dan pengambilan paket data yang sedang melakukan transmisi pada jaringan *wireless LAN*.
- Dengan berhasilnya pengujian *deauthentication attack* maka dari itu dapat dibuktikan bahwa protokol keamanan *WPA1* dan *WPA2* rentan terhadap

serangan *denial of service* atau pemutusan koneksi secara paksa pada jaringan wireless LAN.

- Dengan berhasilnya pengujian *dictionary attack* maka dari itu dapat dibuktikan bahwa paket data *WPA handshake* hasil dari *sniffing packet* pada protokol keamanan *WPA1* dan *WPA2* rentan terhadap serangan *dictionary attack.*

4.1.4 Sistem D

Hasil pengujian pada skenario D yang ditujukan untuk sistem D dengan sub sistem D1, D2, D3 dan D4 menunjukan bahwa tidak semua aktivitas dan serangan pada jaringan *wireless LAN* berhasil dilakukan pada protokol keamanan *WPA1* dan *WPA2* dengan tambahan opsi keamanan *hidden SSID* dan *MAC filtering.* Berikut ini adalah tabel 4.4 berisi tentang rangkuman hasil pengujian skenario D untuk sistem D:

Tabel 4. 4 Rangkuman Pengujian Skenario D untuk Sistem D

Nama Sistem	Protokol Keamanan	Opsi Keamanan	Enkripsi	Panjang Kunci	*Hidden SSID*	*MAC Filtering*
Sistem D1	*WPA1*	*Pre Shared key*	*TKIP*	N/A	ya	ya
Sistem D2	*WPA1*	*Pre Shared key*	AES	N/A	ya	ya
Sistem D3	*WPA2*	*Pre Shared key*	*TKIP*	N/A	ya	ya
Sistem D4	*WPA2*	*Pre Shared key*	AES	N/A	ya	ya

Berdasarkan sistem D1, D2, D3, dan D4 diatas berikut dibawah ini adalah hasil dan status pengujiannya :		
Jenis Pengujian & Serangan	Skenario D	Status Pengujian
	Scanning Wireless Network	Berhasil
	Sniffing Packet	Berhasil
	Deauthentication Attack	Berhasil
	Dictionary Attack	Berhasil
	MAC address Spoofing	Berhasil
	Authentication	Gagal
	Proof Authentication	Gagal

Berdasarkan tabel 4.4 diatas rangkuman hasil semua sistem pengujian dapat diketahui bahwa:

- Dengan berhasilnya pengujian *scanning wireless network* maka dari itu dapat dibuktikan bahwa protokol keamanan *WPA1* dan *WPA2* dengan tambahan opsi keamanan *hidden SSID* dan *MAC filtering* rentan terhadap pencurian informasi terkait dengan identitas sistem dan komponen pada jaringan *wireless LAN*.
- Dengan berhasilnya pengujian *sniffing packet* maka dari itu dapat dibuktikan bahwa protokol keamanan *WPA1* dan *WPA2* dengan tambahan opsi keamanan *hidden SSID* dan *MAC filtering* rentan terhadap pencurian dan pengambilan paket data yang sedang melakukan transmisi pada jaringan *wireless LAN*.
- Dengan berhasilnya pengujian *deauthentication attack* maka dari itu dapat dibuktikan bahwa protokol keamanan *WPA1* dan *WPA2* dengan tambahan opsi keamanan *hidden SSID* dan *MAC filtering* rentan terhadap serangan *denial of service* atau pemutusan koneksi secara paksa pada jaringan wireless LAN.
- Dengan berhasilnya pengujian *dictionary attack* maka dari itu dapat dibuktikan bahwa paket data *WPA handshake* hasil dari *sniffing packet* pada protokol keamanan *WPA1* dan *WPA2* dengan tambahan opsi keamanan *hidden SSID* dan *MAC filtering* rentan terhadap serangan *dictionary attack*.
- Dengan Gagalnya pengujian *Authentication* maka dari itu dapat dibuktikan bahwa protokol keamanan *WPA1* dan *WPA2* dengan opsi keamanan *Pre Shared key* menggunakan enkripsi *TKIP* dan AES dengan konfigurasi *Hidden SSID* dan *MAC Filtering* lebih unggul.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil dari pengujian yang telah dilakukan pada semua sistem dan skenario yang dibuat, berikut ini adalah kesimpulannya :

1. Protokol keamanan *WEP* rentan terhadap serangan *Scanning Wireless Network*, *Sniffing Packet*, *ARP Request Replay Attack*, *Deauthentication Attack*, *Cracking WEP* dan *MAC address* Spoofing..
2. Protokol keamanan *WPA1* dan *WPA2* rentan terhadap serangan *Scanning Wireless Network*, *Sniffing Packet*, *Deauthentication Attack*, *Dictionary Attack* dan *MAC address* Spoofing.
3. Dari protokol keamanan *WEP*, *WPA1* dan *WPA2*, protokol keamanan yang paling unggul untuk digunakan adalah *WPA1* dan *WPA2* dengan opsi keamanan *Pre Shared key* menggunakan enkripsi *TKIP* dan AES dengan konfigurasi *Hidden SSID* dan *MAC Filtering*.

5.2 Saran

Mengingat keterbatasan yang dialami penguji dalam melakukan pengujian, maka dari itu penguji menyarankan penelitian selanjutnya dilakukan pada protokol keamanan *WPA1* dan *WPA2* enterprise menggunakan *RADIUS Server*.

DAFTAR PUSTAKA

Anhar. 2010. *Cara Mudah Mengamankan Data Komputer & Laptop*. Mediakita, Jakarta.

Anonim, *Dictionary attack*. Available at http://en.wikipedia.org/wiki/Dictionary_attack Diakses 4 Oktober 2012.

Anonim, *MAC spoofing*. Available at http://en.wikipedia.org/wiki/MAC_spoofing Diakses 7 Oktober 2012.

D'otreppe, Thomas. 2010. *Aircrack-ng*. Available at http://www.aircrack-ng.org/doku.php?id=aircrack-ng, Diakses 6 Oktober 2012.

D'otreppe, Thomas. 2010. *ARP Request Replay Attack*. Available at http://www.aircrack-ng.org/doku.php?id=arp-request_reinjection, Diakses 5 Oktober 2012.

D'otreppe, Thomas. 2010. *Deauthentication*. Available at http://www.aircrack-ng.org/doku.php?id=deauthentication, Diakses 5 Oktober 2012.

Febrian, Jack. 2004. *Kamus Komputer & Teknologi Informasi*. Informatika, Bandung.

Hiemstra, Johan. 2003. *Tech Exams CompTIA Network +*. TechExam, USA.

Prabawati, Ari. 2010. *Tutorial 5 Hari Belajar Hacking dari Nol*. Andi, Jakarta.

Ramachandran, Vivek. 2011. *BackTrack 5 Wireless Penetration Testing Beginner's Guide*. Paket Publishng, Birmingham - Mumbai.

St'o. 2007. *Wireless Kung Fu Networking & Hacking*. Jasakom, Jakarta.

Utama, Yoga Satria. 2009. *Pengujian Serangan Keamanan Wireless LAN*. Skripsi, FIK UPN Jakarta.

Utapea, Tio Lindung. 2011. *Analisa dan Implementasi Sistem Otentikasi pada Sistem Jaringan Wireless LAN Menggunakan Easyhotspot*. Skripsi, FIK UPN Jakarta.