PERANCANGAN MEKANISME AUDIT KEAMANAN WLAN DENGAN OTENTIKASI RADIUS

LAPORAN TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Teknik Informatika

Disusun Oleh :

Nama : Naufal Aziz

NIM : 06 523 285

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

2011

HALAMAN JUDUL

PERANCANGAN MEKANISME AUDIT KEAMANAN WLAN DENGAN OTENTIKASI RADIUS

LAPORAN TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Teknik Informatika

Disusun Oleh :

Nama : Naufal Aziz
NIM : 06 523 285

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

YOGYAKARTA

2011

LEMBAR PENGESAHAN PEMBIMBING

PERANCANGAN MEKANISME AUDIT KEAMANAN WLAN DENGAN OTENTIKASI RADIUS

LAPORAN TUGAS AKHIR

Disusun oleh

Nama : Naufal Aziz

NIM : 06 523 285

Yogyakarta, 13 Desember 2011

Telah Diterima Dan Disetujui Dengan Baik Oleh :

Dosen pembimbing

_____

Syarif Hidayat, S.Kom., M.I.T.

LEMBAR PENGESAHAN PENGUJI

PERANCANGAN MEKANISME AUDIT KEAMANAN WLAN DENGAN OTENTIKASI RADIUS

TUGAS AKHIR

Disusun oleh:

Nama : Naufal Aziz

NIM : 06 523 285

Telah Dipertahankan di Depan Sidang Penguji Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Teknik Informatika
Fakultas Teknologi Industri Universitas Islam Indonesia.
Yogyakarta, 10 Januari 2012

Tim Penguji

Syarif Hidayat, S.Kom., M.I.T. _____
Ketua

R.Teduh Dirgahayu, ST., M.Sc., Ph.D. _____
Anggota I

Ahmad M. Raf'ie Pratama ST., M.I.T. _____
Anggota II

Mengetahui,
Ketua Jurusan Teknik Informatika
Universitas Islam Indonesia

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

LEMBAR PERNYATAAN KEASLIAN

HASIL TUGAS AKHIR

Saya yang bertanda tangan dibawah ini,

Nama : Naufal Aziz

NIM : 06 523 285

Menyatakan bahwa seluruh komponen dan isi dalam laporan Tugas Akhir ini adalah hasil karya sendiri. Apabila dikemudian hari terbukti bahwa ada beberapa bagian dari karya ini adalah bukan hasil karya saya sendiri, maka saya siap menanggung resiko dan konsekuensi apapun.

Demikian pernyataan ini saya buat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 28 Desember 2011

_____

Naufal Aziz

HALAMAN PERSEMBAHAN

Tugas Akhir ini kupersembahkan untuk

Ibu dan Bapakku

Yang senantiasa memberikan segalanya yang dapat diberikan kepada anak - anaknya

HALAMAN MOTTO

"Sembahlah Allah, dan janganlah kalian mempersekutukan sesuatu apapun dengan-Nya." (**QS. An-Nisaa': 36**)

"Waktu jauh lebih berharga dari pada uang"

KATA PENGANTAR

"*Bissmillahirrohmanirrohim*"

Assalamu'alaikum Wr.Wb.

Allahamdulillahirobbil'alamin, hanya rasa sukur yang sangat mendalam yang dapat penulis panjatkan kehadirat Allah SWT, karena hanya dengan ridho dan hidayahNya penulis dapat menyelesaikan Tugas Akhir yang berjudul "Perancangan Mekanisme Audit Keamanan WLAN Dengan otentikasi RADIUS" sebagai prasyarat untuk menyelesaikan masa pembelajaran jenjang Sarjana Strata 1 di jurusan Teknik Informatika Universitas Islam Indonesia.

Ada banyak sekali pembelajaran yang penulis dapatkan selama proses penyelesaian Tugas Akhir ini, dan tak lupa penulis ucapkan banyak terimakasih terhadapat pihak – pihak yang secara langsung maupun tak langsung terlibat dalam penyelesaian Tugas Akhir ini. Untuk itu penulis ingin mengucapkan ucapan terimakasih yang tulus kepada:

1. Allah SWT atas segala karunia, rahmat dan hidayahNya, juga kepada junjungan kita Nabi besar Muhammad SAW.
2. Nabi Muhammad SAW sebagai utusanNya yang telah menyampaikan dan mengajarkan kebenaran yang hakiki.
3. Ibunda Susilastuti yang tak pernah putus do'a, dukungan dan kasih sayang kepada putra-putrinya.
4. Ayahanda Abdul Aziz yang selalu mengajarkan nilai - nilai kehidupan di dunia maupun di akhirat kelak.
5. Kakakku Nur'aini yang selalu memberi semangat dan dukungan.
6. Bapak Syarif Hidayat, S.Kom., M.I.T., selaku dosen pembimbing yang telah memberikan pengarahan, bimbingan, masukan serta dorongan semangat selama pelaksanaan tugas akhir dan penulisan laporan.
7. Bapak Gumbolo Hadi Susanto, Ir., M.Sc selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia.

8. Bapak Yudi Prayudi, S.Si., M.Kom. selaku Ketua Jurusan Informatika Universitas Islam Indonesia.
9. Seluruh Dosen Jurusan Teknik Informatika Universitas Islam Indonesia yang telah mengajarkan banyak ilmu, dan semoga ilmu yang diberikan menjadi suatu nilai ibadah.
10. Teman - teman "cah nakal", Adit, Miftah, Opek, Indra, Fikri, Arief, Jayong, Warsun, terima kasih atas tawa dan semangat kalian.
11. Teman - teman seperjuangan Cemung, Andra, Andi, Imus, Reza, Yoyok, Galih, semoga kesuksesan selalu bersama kita.
12. Teman - teman divisi Jakal, Pakem, Gamping, Maguwo, Baciro, terimakasih telah menyediakan tempat untuk gelandangan.
13. Saudara - saudari di "*Paguyuban Seni Rukun Rencang*" G1 – G5 yang telah memberi nuansa yang unik. Especially for Mas Aris dan Bang Eri yang telah mewariskan teknik gitar dan sound engineering. "*Speed dan Shreding kalian sungguh joosh*".
14. Teman - teman di Ulil Albab UII dan Pondok. Terutama untuk ustad Ali. Terima kasih atas ilmu yang telah disampaikan. Semoga Ilmu Islam yang kita amalkan sesuai dengan apa yang Rassulullah SAW ajarkan.
15. Teman-teman Teknik Informtika 2006 (FIRE), terimakasih atas pertemanan yang telah kita jalin dan semoga agan terus terjalin.
16. Semua pihak yang telah membantu dalam menyelasikan Tugas Akhir ini.

Semoga Allah SWT senantiasa membalas semua kebaikan dan jasa-jasa yang telah diberikan dengan pahala yang berlimpah, amin.

Akhir kata penulis berharap semoga Tugas Akhir ini dapat menjadi sumber ilmu yang bermanfaat bagi siapa saja yang membacanya.

Yogyakarta, 9 Januari 2012

Naufal Aziz

SARI

Karena fleksibilitasnya WLAN(Wireless Local Area Networks) banyak diimplementasikan, terutama untuk kebutuhan sharing koneksi internet. Disamping kefleksibelan yang diberikan, WLAN sangat terkait dengan isu keamanan. Misalnya penyadapan paket data, pencurian data dan penggunaan oleh pihak ketiga yang tidak berhak. Oleh sebab itu pengelola WLAN/hotspot banyak menerapkan sistem keamanan pada jaringannya. Dari sekian banyak metode keamanan, RADIUS dianggap sebagai metode yang cukup aman. RADIUS (Remote Authentication Dial-In User Service) adalah sebuah protokol keamanan komputer yang digunakan untuk membuat manajemen akses secara terkontrol pada sebuah jaringan. Cara kerja RADIUS secara sederhana adalah melakukan otentikasi, otorisasi, dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan atau biasa disebut AAA (Authentication, authorization, and accounting),sehingga yang menggunakan wireless adalah pengguna yang sah.

Untuk mengetahui seberapa amankah sistem RADIUS, akan dilakukan eksplorasi keamanan terhadap jaringan wireless yang menggunakan sistem RADIUS tersebut. Hasil ekplorasi keamananan akan dijadikan sebagai pertimbangan untuk melakukan audit.

Hasil dari tugas akhir ini adalah mengetahui metode keamanan dan audit sistem RADIUS pada jaringan wireless.

Kata kunci :
WLAN, RADIUS, AAA

TAKARIR

Account	Akun pada sistem
administrator	Pemegang hak kekuasaan penuh
arp poisioning	Serangan pada arp
Attacker	Pihak yang melakukan serangan
Billing plan	Aturan pada billing
Broadcast	Disebarkan ke semua
Browser	Aplikasi untuk menjelajah internet
Bypass	Melewati suatu sistem keamanan
Capture	Menangkap atau melihat paket data
Challenge	Kode acak
Channel	Kanal frekuensi
Chipset	IC kecil pada perangkat komputer
Coverage area	Ruang yang dapat dicakup
Default	Konfigurasi awal bawaan
Denial of service	Salah satu kategori serangan jaringan
Device	Alat atau piranti
Disable	Membuat jadi tidak aktif
Driver	perangkat lunak untuk menjalankan hardware
Enkripsi	Pengacakan data
fake AP	Access point palsu
Firewall	Penyaring paket jaringan
Forward	Meneruskan paket data
Gateway	Penghunung internal ke eksternal
Generate	Proses pembentukan
Hacking	Kegiatan merusak sistem
Hardware	Perangkat keras komputer
Hotspot	Tempat layanan internet dengan media wireless
Interface	Pintu masuk pada jaringan komputer

IP address	Alamat jaringan
Isolation	Perlindungan pada sinyal
Jamming	Gangguan pada sinyal wireless
Localhost	Komputer yang sedang dipakai
Login	Masuk ke dalam sistem
MAC address	Penanda atau alamat hardware
Man in the middle attack	Salah satu tipe serangan jaringan
Network access server	Gateway client dari RADIUS server
Noise	Sinyal pengganggu
Opensource	Software gratis dengan kode yang terbuka
Output	Hasil keluaran
Packetbased	Perhitungan berdasarkan besarnya paket data
Passive sniffing	Metode menyadap data
Posting	Mengirimkan data
Postpaid	Pasca bayar
Pre-Shared Key	Salah satu sistem keamanan wireless
Privacy	Data penting yang bersifat pribadi
Promiscuous mode	Mode menerima semua paket data
Protokol	Standar aturan untuk berkomunikasi
Record	Baris data pada database
Redirect	Pengalihan ke alamat tertenetu
Relay	Meneruskan sinyal
Repeater	Alat untuk memperkuat sinyal
Request For Comment	Standar yang digunakan dalam internet
Request	Permintaan
Risk	Resiko keamanan
Root	Hak akses tertinggi
Rouge AP	Access point palsu
Router	Penghubung antar jaringan
Script	Kode program komputer
Server	Penyedia layanan jaringan

Shared secret	Karakter yang digunakan untuk enkripsi
Sharing	Berbagi data
Sniffer	Perangkat atau aplikasi penyadap data
Sniffing	Menyadap data
Spoofing	Pemalsuan data
Timebased	Perhitungan berdasarkan waktu
Tools	Alat atau piranti
Traffic	Lalulintas jaringan
User	Pengguna sistem
Virtual	Interface interface buatan
Virus	Aplikasi yang bersifat merusak
Wi-Fi Protected Access	Salah satu sistem keamanan wireless
Wired Equivalent Privacy	Salah satu sistem keamanan wireless
Wired	Menggunakan kabel
Wireless Access Point	Alat penghubung jaringan wireless
Wireless card	Kartu jaringan wireless
Wireless router	Router sekaligus access point
Wireless	Tanpa kabel

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Wireless Local Area Network (WLAN) banyak diemplementasikan terutama untuk kebutuhan *sharing* koneksi internet dikarenakan penggunaannya yang mudah. WLAN adalah suatu jaringan lokal tanpa kabel yang menggunakan gelombang radio sebagai media tranmisinya. WLAN dibuat berdasar atas spesifikasi IEEE 802.11.

Disamping kemudahan yang diberikan, WLAN sangat terkait dengan isu keamanan, mulai dari penyadapan pengiriman paket data, pencurian data, hingga penggunaan oleh pihak ketiga yang tidak mempunyai hak. Hal-hal tersebut membuat banyak pengelola WLAN menerapkan sistem keamanan pada jaringannya. Metode-metode keamanan dalam WLAN cukup banyak, antara lain dapat menggunakan *Wired Equivalent Privacy*(WEP), *Wi-Fi Protected Access* (WPA), *Pre-Shared Key* (PSK), dan *Remote Authentication Dial-In User Service* (RADIUS). Metode-metode keamanan tersebut memiliki beberapa kelebihan dan kekurangan, RADIUS dianggap memiliki tingkat keamanan yang baik.

RADIUS adalah sebuah protokol keamanan yang digunakan untuk membuat manajemen akses secara terkontrol pada sebuah jaringan. Cara kerja RADIUS secara sederhana adalah melakukan autentikasi, otorisasi, dan pendaftaran pengguna secara terpusat untuk mengakses jaringan atau biasa disebut *Authentication, Authorization, and Accounting* (AAA). Sistem tersebut mengharuskan pengguna melewati mekanisme *login* terlebih dahulu.

Penerapan sistem otentikasi dan otorisasi koneksi user dengan menggunakan Chillispot dan server Radius memberikan level keamanan jaringan komputer wireless yang lebih baik. User yang dapat menggunakan layanan jaringan harus terdaftar dalam sistem sehingga tidak semua orang dapat menggunakan layanan jaringan (SNATI, 2006).

Faktanaya tidak ada sistem yang 100% aman, dari itu dilakukan audit pada sistem RADIUS.

1.2 Rumusan Masalah

Bagaimana membuat *checklist* audit untuk meningkatkan keamanan WLAN dengan sistem RADIUS.

1.3 Batasan Masalah

Dalam melaksanakan suatu penelitian, diperlukan adanya batasan agar tidak menyimpang dari yang telah direncanakan sehingga tujuan yang sebenarnya dapat tercapai. Adapun batasan masalah dalam tugas akhir ini antara lain:

1. Alat yang digunakan hanya mendukung WLAN 802.11 b/g.
2. WLAN yang digunakan yang digunakan pada penelitian ini tidak menggunakan mekanisme enkripsi

1.4 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat membantu pengelola WLAN untuk mengetahui cara kerja dan celah-celah keamanan RADIUS.

1.5 Metodologi Penelitian

Metode yang digunakan dalam penelitian ini adalah :

1. Membuat topologi jarigan.
2. Instalasi dan konfigurasi.
3. Melakukan autentikasi antara *user* dengan *server* RADIUS.
4. Memonitoring kegiatan otentikasi.
5. Analisa paket data RADIUS.
6. Melakukan pengujian dengan serangan terhadap keamanannya.
7. Audit keamanan jaringan komputer.

1.6 Sistematika Penulisan

Bab I mendefinisikan latar belakang masalah yaitu tentang RADIUS yang banyak diimplementasikan ternyata masih mempunyai celah – celah keamanan. batasan masalah terbatas pada penggunaan RADIUS untuk mendukung keamanan pada jaringan *wireless*. Bab ini juga memuat rumusan masalah, manfaat dari penelitia, metodologi penelitian dan sistematika penulisan laporan.

Bab II membahas dasar-dasar teori yang digunakan dalam penelitian yaitu membahas secara singkat tentang LAN, WLAN, *captiveportal*, RADIUS dan macam – macam insiden keamanan jaringan.

Bab III menjabarkan langkah-langkah yang nantinya digunakan dalam penelitian yang meliputi metode analisis, perangkat lunak yang digunakan, perangkat keras yang dibutuhkan, topologi jaringan serta tahapan eksplorasi terhadap keamanan sistem.

Bab IV menjabarkan hasil dari penelitian yaitu tahap instalasi dan konfigurasi sistem, hasi pengujian terhadap keamanan dan audit sistem RADIUS.

Bab V berisi kesimpulan dari hasil penelitian dan saran untuk memperbaiki, mengembangkan ataupun untuk memberikan solusi dari masalah – masalah yang muncul dalam penelitian.

BAB II
LANDASAN TEORI

2.1 Local Area Network

Local Area Network (LAN) merupakan jaringan privat di dalam sebuah bangunan yang memiliki ukuran jarak sampai beberapa kilometer. LAN digunakan untuk menghubungkan komputer-komputer dan *workstation* untuk memakai resource secara bersama-sama dan saling bertukar informasi.

LAN seringkali menggunakan teknologi transmisi kabel tunggal. LAN tradisional beroperasi pada 10 hingga 100 Mbps dengan delay puluhan microsecond dan memiliki faktor kesalahan kecil. Sedangkan LAN modern beroperasi pada kecepatan yang lebih tinggi, hingga ribuan Mbps.

2.2 Wireless Local Area Network

Wireless Local Area Network (WLAN) merupakan LAN tanpa kabel yang menggunakan gelombang elektromagnet sebagai media tranmisinya. WLAN menggunakan standar spesifikasi IEEE 802.11.

Pada WLAN terdapat 4 standar yang populer yaitu 802.11a, 802.11b, 802.11g, dan 802.11n.

Tabel 2.1 Spesifikasi WLAN

Spesifikasi	Kecepatan	Frekuensi	kecocokan
802.11a	54 Mb/s	5 GHz	a
802.11b	11 Mb/s	2,4 GHz	b
802.11g	54 Mb/s	2,4 GHz	b, g
802.11n	100 Mb/s	2,4 GHz, 5 GHz	b, g, n

2.3 Captive Portal

Captive Portal adalah suatu teknik otentikasi dan pengamanan data yang lewat dari jaringan internal ke jaringan eksternal. *Captive Portal* sebenarnya merupakan mesin *router* atau *gateway* yang memproteksi atau tidak mengizinkan adanya *traffic* hingga pengguna melakukan registrasi. Biasanya *Captive Portal* ini digunakan pada infrastruktur *wireless* seperti *hotspot*, tapi tidak menutup kemungkinan diterapkan pada jaringan kabel.

Cara kerja *Captive Portal* adalah pada saat seorang pengguna berusaha untuk melakukan browsing ke Internet, *captive portal* akan memaksa pengguna yang belum terotentikasi untuk menuju ke halaman *login*yang berada di web server internalnya.*Router/wireless gateway* mempunyai mekanisme untuk menghubungi sebuah *Authentication server* untuk mengetahui identitas dari pengguna wireless yang tersambung. Dengan demikian*wireless gateway* dapat menentukan untuk membuka aturan *firewall*-nya untuk pengguna tertentu.

2.4 RADIUS

Remote Authentication Dial-In User Service (RADIUS) adalah sebuah protokol keamanan jaringan komputer yang digunakan untuk membuat manajemen akses secara terkontrol pada sebuah jaringan. RADIUS melakukan *Authentication, Authorization, Accounting* (AAA).

Authentication yaitu memastikan apakah pelanggan telah terdaftar pada sebuah jaringan. RADIUS menggunakan RSA Secure ID untuk membuat autentikasi yang kuat dalam pengontrolan akses. Autentikasi RADIUS menggunakan port 1812.

Authorization yaitu mengetahui hak akses pengguna, apakah hanya sebagai pelanggan atau sebagai administrator, sehingga pengguna akan mendapatkan layanan berbeda-beda sesuai dengan hak aksesnya dan jaringan menjadi lebih terkontrol. Sedangkan *Accounting* adalah pendaftaran *account.* Pengguna yang inigin mendapatkan layanan jaringan harus didaftarkan terlebih dahulu pada sistem RADIUS. *Accounting* biasanya menggunakan port 1813 namun ada juga vendor yang menggunakan port 1645/1646 (cisco) dan 1645/1646 (juniper).

RFC (*Request For Comment*) yang berhubungan dengan RADIUS diantaranya:

RFC2865 : *Remote Authentication Dial-In User Service* (RADIUS)

RFC 2866 : RADIUS *Accounting*

RFC 2867 : RADIUS *Accounting for Tunneling*

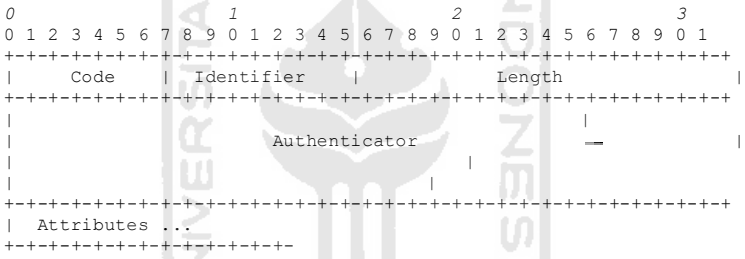
RFC 2868 : RADIUS *Authentication for Tunneling*

RFC2869 : RADIUS *Extensions*

RFC 3162 : RADIUS *over IP6*

RFC 2548 : Microsoft Vendor-Specific RADIUS *Attributes*

RADIUS berbasis pada protokol UDP. RADIUS mempunyai struktur paket data yang terdiri dari 5 bagian pokok, yaitu *code*, *identifier*, *length*, *authenticator*, dan *attributes.* Ilustrasi paket data RADIUS dapat dilihat pada gambar 2.1 di bawah ini:



Gambar 2.1 Struktur Paket Data RADIUS

1. *Code*

Code digunakan untuk membedakan tipe pesan RADIUS yang dikirimkan pada paket. *Code* memiliki panjang satu oktet. *Code* inilah yang akan menentukan tipe paket data RADIUS.

2. *Identifier*

Identifier memiliki panjang satu oktet. *Identifier* berfungsi untk mencocokkan *requests* dan *replies.*

3. *Length*

Length memiliki panjang dua oktet. *Length* berfungsi untuk mengindikasikan panjang keseluruhan paket. *Range* dari *length* adalah 20 – 4096. Paket yang memiliki panjang paket di luar *range* tersebut akan diabaikan.

4. *Authenticator*

Authenticator Memiliki panjang 16 oktet. *Authenticator* digunakan untuk mencocokkan balasan dari *server* RADIUS, selain itu digunakan juga untuk algoritma password.

5. *Attributes*

Attributes digunakan untuk menyimpan detil informasi dan konfigurasi RADIUS. *field attributes* dapat berisi lebih dari satu *value*. Contoh *value* dari a*ttributes* dapat dilihat di tabel 2.3 berikut.

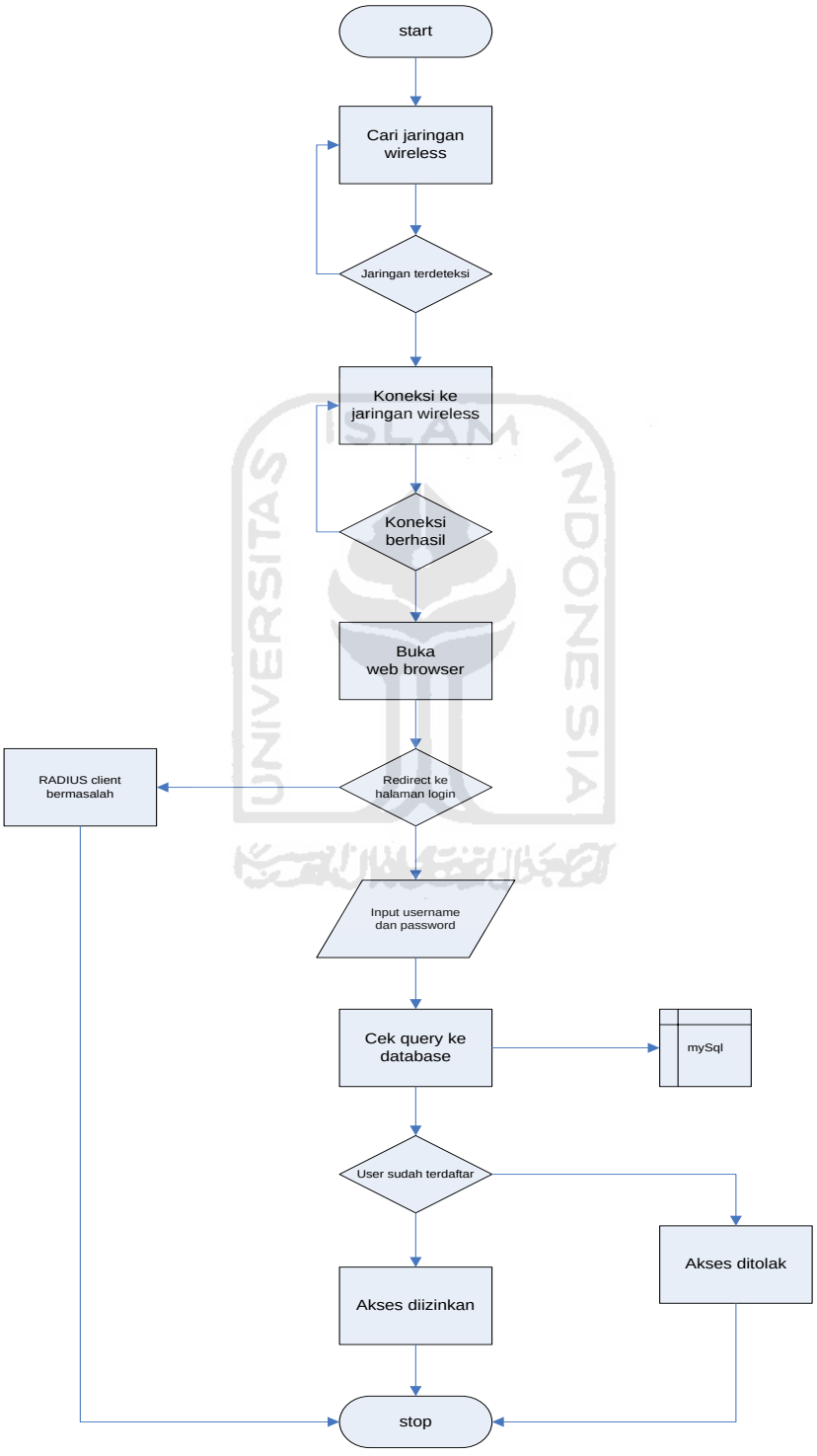
Tabel 2.2 Tabel Attributes RADIUS

value	***Description***
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
9	Framed-IP-Netmask
10	Framed-Routing
11	Filter-Id
12	Framed-MTU
13	Framed-Compression
14	Login-IP-Host
15	Login-Service
16	Login-TCP-Port
17	(unassigned)
18	Reply-Message

19	Callback-Number
20	Callback-Id
21	(unassigned)
22	Framed-Route
23	Framed-IPX-Network
24	State
25	Class
26	Vendor-Specific
27	Session-Timeout
28	Idle-Timeout
29	Termination-Action
30	Called-Station-Id
31	Calling-Station-Id
32	NAS-Identifier
33	Proxy-State
34	Login-LAT-Service
35	Login-LAT-Node
36	Login-LAT-Group
37	Framed-AppleTalk-Link
38	Framed-AppleTalk-Network
39	Framed-AppleTalk-Zone
40-59	(reserved for accounting)
60	CHAP-Challenge
61	NAS-Port-Type
62	Port-Limit
63	Login-LAT-Port

2.5 Cara Kerja RADIUS

Berikut ini adalahgambaran umum proses user yang mengakses wireless dengan sistem RADIUS.



Gambar 2.2 Cara Kerja RADIUS

Pada gambar diatas dapat dilihat tentang bagaimana RADIUS melakukan otentikasi pada setiap user(*wirelessclient*) yang mencoba masuk ke dalam jaringan *wireless*.Setiap user yang melakukan koneksi melalui jaringan wireless dan mencoba untuk browsing internet, akan di – redirect ke halaman login chillispot. Di halaman login tersebut user diminta untuk mengisi username dan password. Kemudian chillispot menanyakan ke FreeRADIUS apakah username dan password tersebut valid. FreeRADIUS mencocokkan username dan password tersebut dalam databasenya di MySql. Jika cocok FreeRADIUS akan mengirim pesan ke chillispot untuk mengizinkan user melakukan koneksi ke internet. Jika username dan password tidak cocok, FreeRADIUS mengirimkan pesan ke chillispot bahwa username dan password tersebut tidak valid. Chillispot tidak akan mengizinkan koneksi ke internet dan meminta user melakukan proses login ulang.

2.6 Insiden Keamanan Jaringan

Insiden keamanan jaringan adalah suatu aktivitas pada suatu jaringan komputer yang memberikan dampak padaap keamanan sistem yang secara langsung atau tidak bertentangan dengan sistem keamanan pada jaringan tersebut. Secara garis besar, insiden dapat diklasisifkasikan menjadi: *proble, scan, account compromize*, *root compromize, packet sniffer,* DOS (D*enial of Service*), *exploitation of trust*. *malicious code* dan *insfrastrucure attack*.

2.6.1 Probe

Sebuah *probe* dapat dikenali dari adanya usaha-usaha yang tidak lazim untuk memperoleh akses ke dalam suatu sistem yang salah salah satu tujuannya adalah berusaha menemukan informasi tentang sisitem tersebut. Salah satu contohnya adalah usaha untuk login ke dalam sebuah *account* yang tidak digunakan. *Probing* ini dapat dianalogikan sebagai usaha untuk memasuki sebuah ruangan, dengan mencoba–coba untuk mengetahui apakah pintu tersebut dikunci atau tidak.

2.6.2 Scan

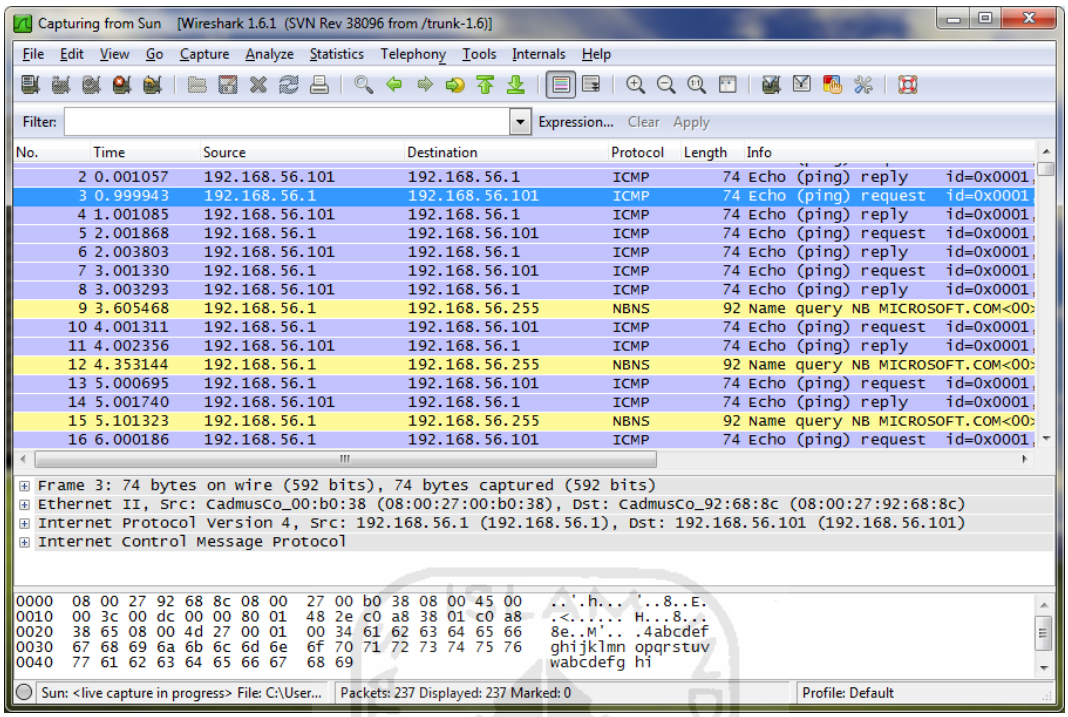
Scan adalah kegiatan *probe* dalam jumlah yang besar dengan menggunakan *tool* secara otomatis. Aplikasi tersebut secara otomatis dapat mengetahui port-port yang terbuka pada host lokal maupun remote. IP address yang aktif, bahkan bisa untuk mengetahui sistem operasi yang digunakan host tujuan. Salah satu contohnya adalah dengan menggunakan aplikasi Nmap.

```
Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-15 12:03 WIT
Nmap scan report for 192.168.182.3
Host is up (0.031s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3306/tcp open  mysql
MAC Address: 00:1C:BF:6A:A1:69 (Intel Corporate)

Nmap scan report for 192.168.182.4
Host is up (0.033s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:16:EA:4F:E1:EE (Intel)
```

Gambar 2.3 Scanning Nmap

2.6.3 Packet Sniffer

Paket sniffer adalah suatu *device*, baik perangkat lunak maupun perangkat keras yang digunakan untuk memperoleh infomasi yang melewati jaringan komputer. kegunaan dari *packet sniffer* adalah membuat NIC (*Network Interface Card*) dapat menangkap semua *traffic* yang perjalan pada suatu jaringan. Mode *promiscuous* adalah mode di mana semua workstation pada sistem jaringan dapat menangkap semua *traffic* yang dialamatkan pada workstation itu sendiri dan juga workstation-workstation lain yang berada di sekitarnya. Contohnya adalah Wireshark.



Gambar 2.4 Wireshark

2.6.4 Account Compromize

Account compromise adalah penggunaan *account* sebuah komputer secara ilegal oleh seseorang yang bukan pemilik *account* tersebut. *Account compromise* dapat mengakibatkan korban mengalami kehilangan atau kerusakan data. Sebuah insiden *account compromise* dapat berakibat lebih lanjut, yaitu terjadinya insiden *root compromise*, yang dapat menyebabkan kerusakan yang lebih besar

2.6.5 Denial of Service

Banyak yang menyebabkan terjadinya DoS, serangan ini berbahaya dikarenakan dapat melumpuhkan koneksifitas antara jaringan yang disebabkan oleh banjirnya *traffic* ataupun juga adanya kemungkinan virus dan menyebabkan sistem komputer menjadi lamban dan bahkan lumpuh. Kemungkinan yang terakhir adalah *device* yang melindungi jaringan rusak. Contoh dari serangan ini adalah *ping of death*, yaitu melakuakan ping dengan jumlah bytes yang besar dan secara terus menerus.

2.7 Audit WLAN

Penggunaan wireless menawarkan berbagai kemudahan dan lebih fleksibel. Akan tetapi di sisi lain resiko yang ditimbulkan juga lebih besar dari pada jaringan wired. Oleh karena itu perlu dilakukan upaya untuk menjamin keamanannya. Salah satunya adalah dengan melakukan audit. Audit secara umum merupakan kegiatan pengawasan dan pengendalian. Audit pada sebuah sistem diharapkan dapat mengoptimalkan kinerja, meminimalkan kesalahan dan memperkuat keamanan pada sistem tersebut.

Salah satu metode penerapan audit adalah dengan menggunakan *checklist*. Berikut ini adalah contoh salah satu standar *checklist*yang diterbitkan oleh SANS IT Audit pada "*Auditing a Cisco Aironet Wireless Network From an Auditors Perspective*". Dalam acuan tersebut, hal – hal yang perlu diperhatikan adalah :

1. Apakah auditor telah mendapatkan izin untuk melakukan audit(subjektif).
2. Apakah dalam institusi tersebut terdapat aturan khusus tentang penggunaan WLAN (subjektif).
3. Pastikan *broadcast* SSID dimatikan
4. Pastikan SSID tidak menggunakan kata yang sepele
5. Pastikan WEP telah diaktifkan.
6. Pastikan MAC *address* filtering telah diaktifkan.
7. Pastikan access point tidak menggunakan power yang berlebihan
8. Pastikan access point diletakkan di tempat yang aman
9. Pastikan password default admin access point telah dirubah
10. Pastikan menggunakan software dan firmware terbaru dan matikan semua *service* yang tidak diperlukan
11. Pastikan sinyal wireless tidak menyebar jauh melebihi area yang ditentukan
12. Selalu lakukan pengecekan terhadap kemungkinan keberadaan *rouge access point*
13. Pastikan konfigurasi jaringan pada access point telah diubah dari default
14. Gunakan otentikasi yang kuat seperti RADIUS
15. Gunakan skema enkripsi yang kuat (misal VPN) untuk menutupi kelemahan WEP

16. Matikan *accesspoint* jika sedang tidak digunakan
17. Matikan fitur DHCP pada *accesspoint* dan gaunakan pengalamatan IP manual pada *clientwireless*
18. Matikan SNMP jika tidak dibutuhkan
19. Gunakan *firewall* diantara jarigan wireless dan jaringan internal
20. Ubah *channeldefault.*

BAB III
METODOLOGI

3.1 Metode Analisis

Analisis dimulai dengan memilih perangkat keras dan perangkat lunak yang dibutuhkan, membuat topologi untuk menerapkan sistem RADIUS, dan melakukan eksplorasi yang berkaitan dengan keamanan sistem tersebut.

3.1.1 Perangkat Lunak yang Dibutuhkan

Perangkat lunak yang dibutuhkan dalam implementasi keamanan RADIUS pada WLAN adalah sebagai berikut :

a. Easyhotspot

Dalam mengimplementasikan sistem RADIUS, sistem operasi yang digunakan adalah Easyhotspot versi 2b. Alasan pemilihan sistem operasi ini untuk dijadikan server RADIUS karena dalam Easyhotspot sudah terpasang freeradius, mysql, httpd dan manajemen sistem RADIUS berbentuk aplikasi web base.

Berikut ini adalah spesifikasi easyhotspot versi 2b :

1. Ubuntu Server 9.04 kernel 2.6.28-15-server
2. FreeRADIUS v2.1.0
3. Chillispot 1.0
4. Apache/2.2.11
5. Mysql 5.0.75-0ubuntu10.2
6. PHP 5.2.6-3ubuntu4.2 with Suhosin-Patch 0.9.6.2 (cli) and Zend Engine v2.2.0
7. Billing Hotspot (CI)

b. Wireshark

wireshark adalah sebuah *Network Packet Analyzer* berbasis *opensource*. Diperlukan untuk menangkap paket – paket jaringan dan berusaha menampilkan semua informasi yang ada di paket – paket tersebut sedetail mungkin.

3.1.2 Perangkat Keras yang Dibutuhkan

a. komputer server RADIUS

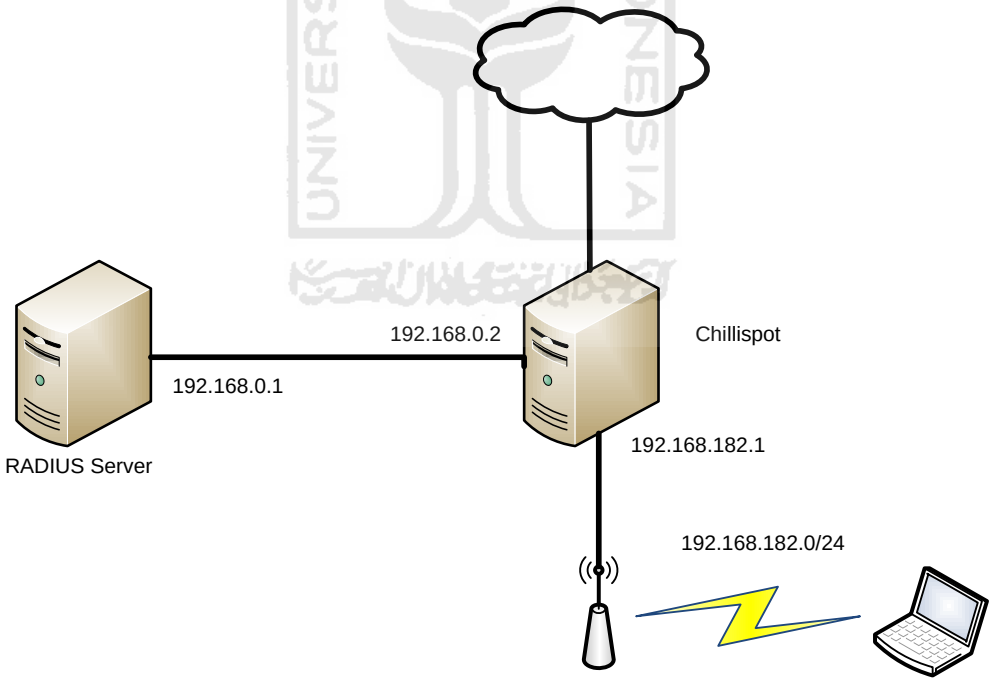
Persyaratan hardware minimum untuk Easyhotspot :

1. Puentium 3 atau setara
2. 512 MB RAM
3. 5 GB Free Space HDD
4. LAN Card

b. Wireless Access Point (tidak perlu menggunakan wireless router)

c. WLAN Card di sisi client

3.1.3 Topologi Jaringan



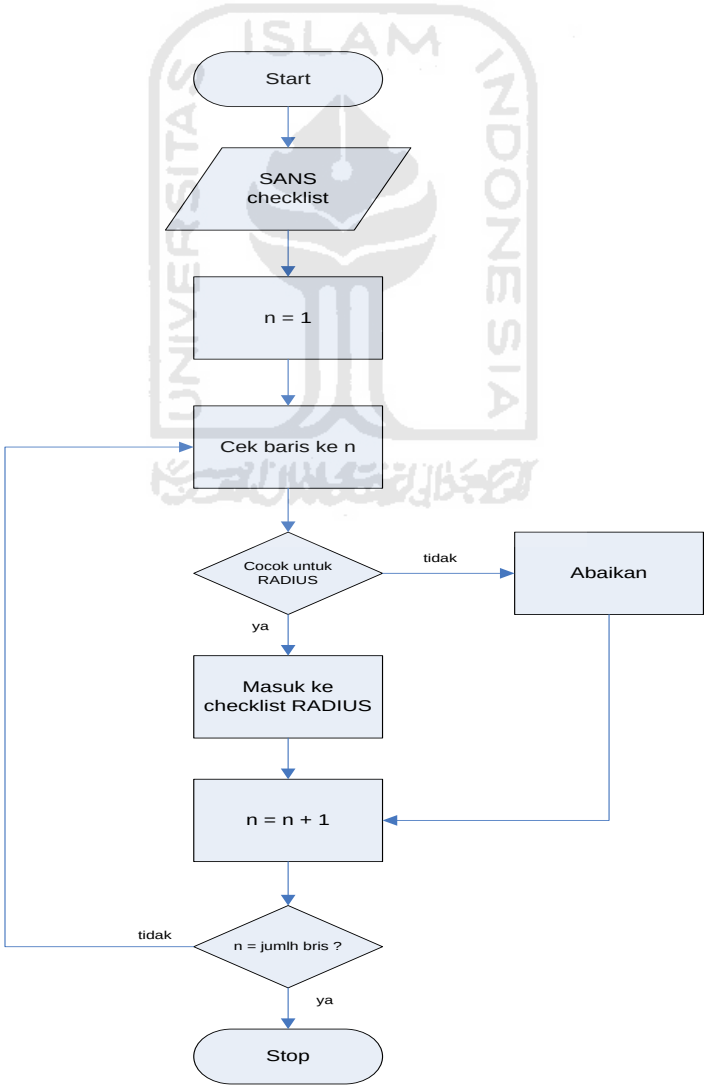
Gambar 3.1 Topologi Jaringan

3.2 Eksplorasi Keamanan

Tahapan pengujian keamanan yang dilakuakan adalah :

1. Monitoring jaringan wireless antara AP dan Client Hotspot dengan airmon-ng dan wireshark.
2. Memantau proses otentikasi*userwireless* pada web browser.
3. Melakukan ARP *spoofing* dengan arpspoof.
4. Menganalisa paket *Acces–Request RADIUS*
5. *Bypass* otentikasi dengan MAC *spoofing*

3.3 Audit Sistem RADIUS



Gambar 3.2 Checklist audit RADIUS

Melalui acuan yang ada pada SANS *checklist*, akan dibentuk *checklist* baru yang sesuai untuk melakukan audit pada sistem RADIUS. *Checkpoint* yang dinilai tidak sesuai untuk sistem RADIUS akan diabaikan. *Cheklist* yang dibentuk juga mempertimbangkan hasil dari eksplorasi keamanan yang dilakukan. Sehingga *checklist* baru yang terbentuk diharapkan dapat meningkatkan keamanan dari sistem RADIUS

BAB IV
HASIL DAN PEMBAHASAN

Hasil dan pembahasan Analisis keamanan RADIUS pada WLAN ditujukan untuk mengetahui bagaimana cara kerja sistem RADIUS yang diimplementasikan dalam mengamankan jaringan *wireless* menganalisa protokol RADIUS terutama pada proses autentikasinya.

4.1 Instalasi dan Konfigurasi

Langkah – langkah yang dilakukan dalam proses instalasi dan konfigurasi adalah sebagai berikut :

4.1.1 Instalasi Easyhotspot

Proses instalasi Easyhotspot adalah sama seperti instalasi Ubuntu pada umumnya. Easyhotspot berfungsi sebagai RADIUS server. Secara *default* freeradius yang ada didalamnya sudah terkonfigurasi untuk melayani *client localhost.* Jika akan menggunakan NAS dari mesin lain maka yang perlu dilakuakan adalah menambah client list yang ada di clients.conf.

Edit file /etc/freeradius/clients.conf. Tambahkan baris berikut :

```
client 192.168.0.2/24 {
  secret    = easyhotspot
}
```

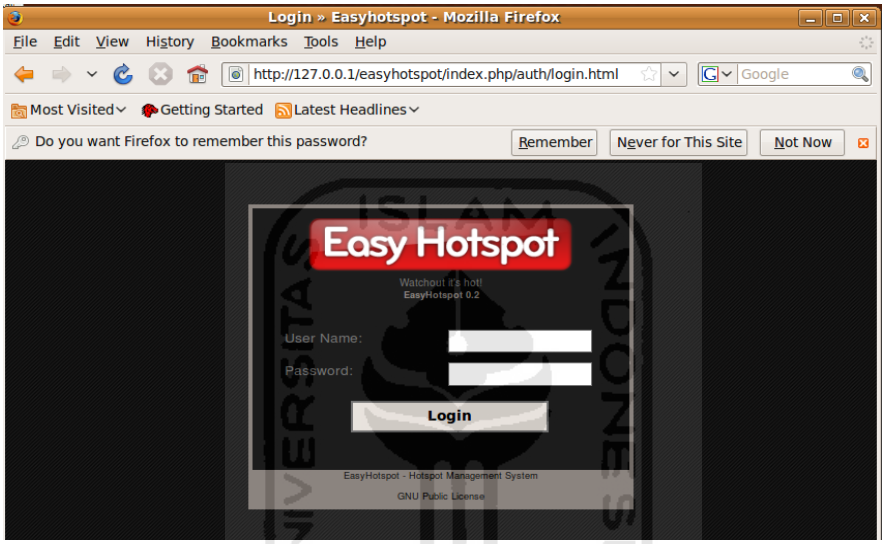
192.168.0.2 adalah IP yang akan dijadikan sebagai NAS dalam kasus ini adalah komputer yang diinstal Chillispot. Secret adalah *key* yang digunakan oleh FreeRadius dan Chillispot untuk berkomunikasi.

4.1.2 Membuat Akun RADIUS

Akun dibedakan menjadi dua macam yaitu *voucher* dan *postpaid.* Pada dasarnya prinsip kedua jenis akun ini adalah sama yaitu untuk membatasi *traffic*

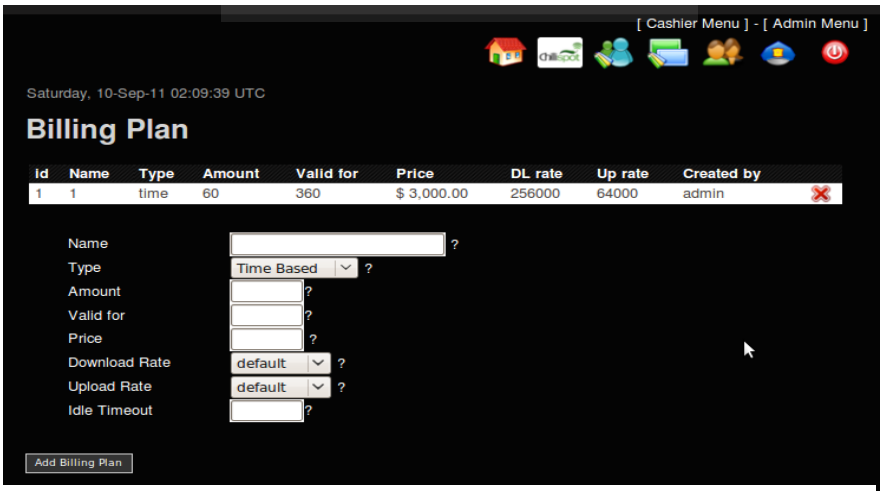
client. Perbedaannya terletak pada metode yang digunakan. Jika menggunakan *voucher* maka waktu penggunaan, besarnya *traffic* dan harga ditentukan di awal, sedangkan jika menggunakan *postpaid* maka biaya akan dihitung di akhir penggunaan. Berikut ini akan dilakukan simulasi pembuatan akun dengan kedua tipe akun tersebut dengan menggunakan easyhotspot web base.

Untuk membuat *voucher* terlebih dahulu harus dibuat *Billing Plan*. Loginlah sebagai admin.



Gambar 4.1 Halaman Login Easyhotspot

Setelah berhasil login, pilih menu *billing plan* dan buat *billing plan* baru.



Gambar 4.2 Billing Plan

Keterangan Gambar 4.2 :

Name : nama dari billing plan.

Type : mendefinisikan tipe yang digunakan yaitu *timebased*(berdasarkan waktu) dan *quotabased*(berdasarkan besar *quota*).

Ammount : waktu penggunaan dalam menit.

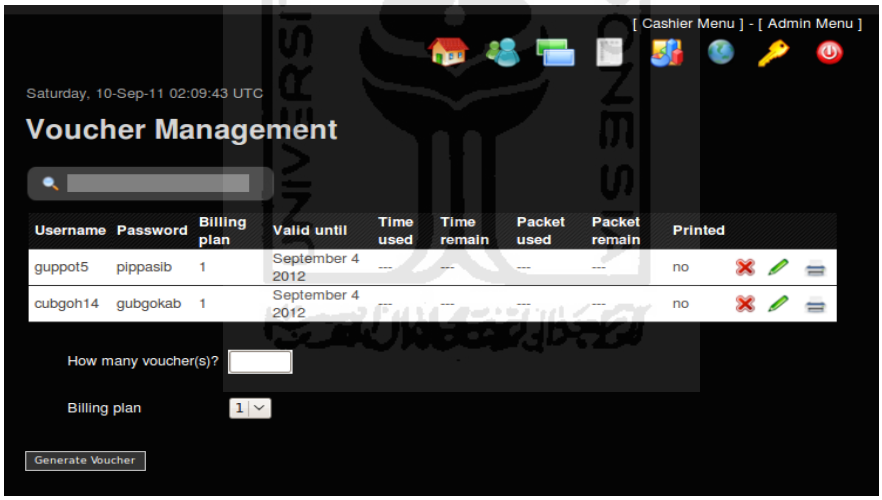
Price : harga voucher

Downloadrate : untuk membatasi kecepatan *download*

Uploadrate : untuk membatasi kecepatan *upload*

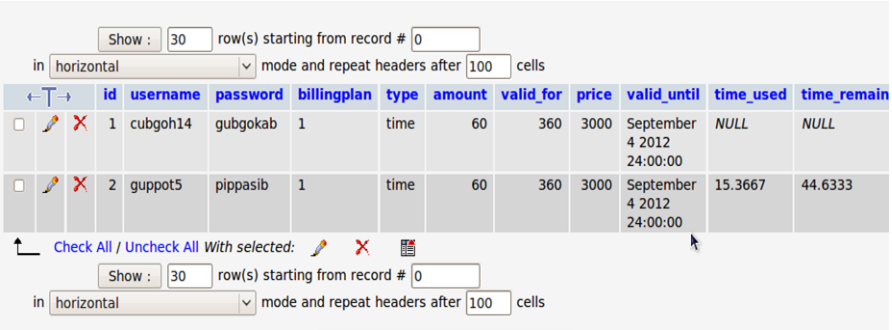
Idletimeout : batas waktu maksimal *client* yang tidak melakukan kegiatan(dalam satuan menit). Jika melebihi batas waktu tersebut sistem dengan sendirinya akan memutuskan koneksi.

Setelah billing plan dibuat, *voucher* sudah bisa dibuat dengan masuk ke*chashiermenu* dan pilih menu *vouchermanagement*



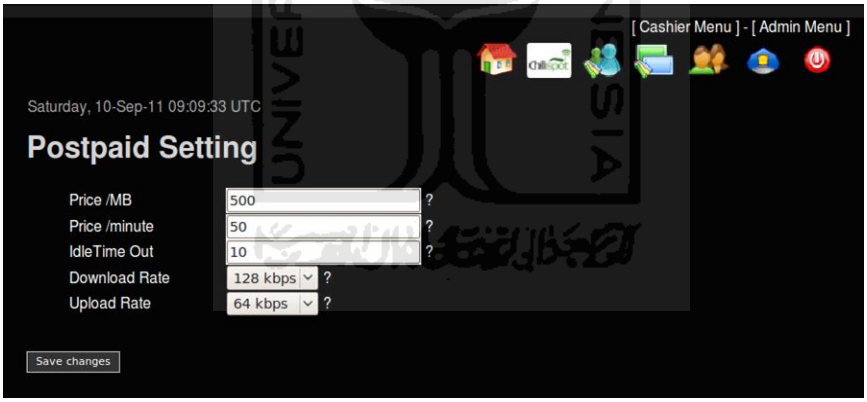
Gambar 4.3 Voucher Management

Setelah *voucher* dibuat, *user* dapat menggunakannya untuk *login* pada sistem. Akun *voucher* tersebut dicatat pada tabel **radiususergroup**, **voucher** dan **voucher_list**. *Billingplan* disimpan pada table **billingplan** di dalam database easyhotspot.



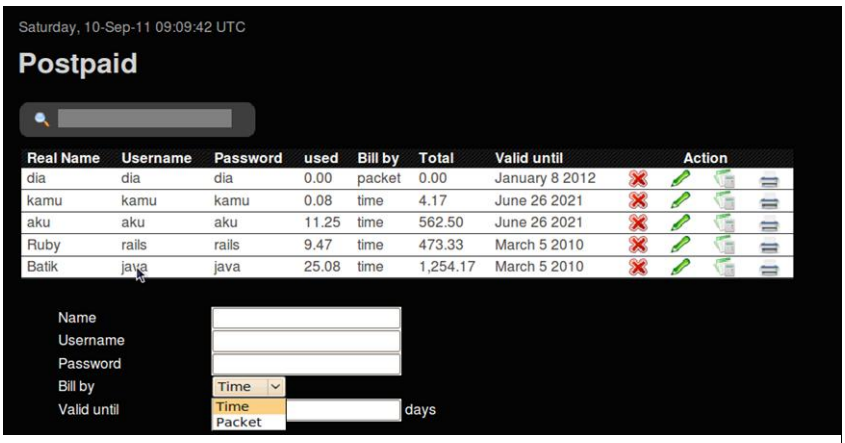
Gambar 4.4 Tabel voucher_list

Untuk akun tipe *postpaid* juga dibedakan berdasarkan waktu dan besarnya paket data. Langkah pertama adalah menentukan biaya yang akan dibebankan pada akun *postpaid*. Login sebagai admin lalu masuk ke menu *accountplan*. Pada menu accountplan terdapat postpaidsetting yang berfungsi untuk menentukan beban biaya yang akan dibebankan kepada akun *postpaid*.



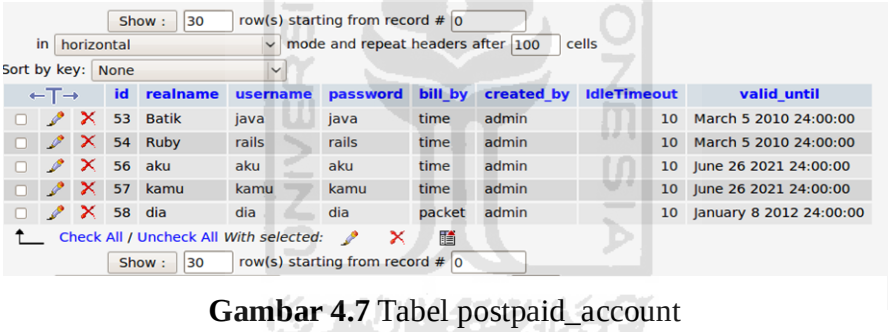
Gambar 4.5 Postpaid Setting

Pada menu postpaidsetting terdapat pengaturan biaya baik untuk *timebased* ataupun *packetbased*. Setelah biaya telah ditentukan, langkah berikutnya adalah membuat akun *postpaid* itu sendiri. Masuk ke *cashiermenu* lalu pilih *postpaidmenu* dan buat akun baru. Pada *postpaidmenu* terdapat dua pilihan tipe akun yaitu *timebased* dan *packetbased*. Besarnya biaya yang dikenakan mengikuti *postpaidsetting* yang telah ditetapkan oleh administrator.



Gambar 4.6 Postpaid

Data akun *postpaid* dicatat pada tabel **postpaid_account**, **postpaid_account_bill**, **postpaid_account_list** dan data *postpaid setting* pada tabel **postplan**.



Gambar 4.7 Tabel postpaid_account

Berikut ini adalah tabel – tabel utama yang digunakan oleh Freeradius :

1. nas

   berfungsi untuk menyimpan data RADIUS *client* yang berhak berkomunikasi dengan RADIUS *server*.

2. radacct

   berperan dalam proses *accounting* utama freeRADIUS. Tabel ini mencatat semua data *wirelessclient* yang telah terkoneksi dengan freeRADIUS.

3 radcheck

   berfungsi mencatat pengecekan yang dilakukan oleh RADIUS *server* terhadap setiap *access-request* yang masuk.

4 radgroupcheck

berfungsi membatasi akses dari suatu *groupname*(*groupname* terbentuk dari billingplan yang digunakan untuk membuat voucher).

5 radgroupreply

berfungsi untuk me-*replymessage* kepada suatu *groupname*.

6 radpostauth

berfungsi menyimpan *reply-Message* dari *wireless* client pada proses autentikasi.

7 radreply

berfungsi sama seperti **radgroupcheck** tetapi digunerakan untuk me-*reply message* terhadap seorang *user wireless* sehingga tiap – tap *user* bisa diberi batasan akses.

8 radusergroup

berfungsi untuk menyimpan data *user* yang tergabung dalam suatu *groupname*.

4.1.3 Instalasi Chillispot

Peran Chillispot adalah sebagai NAS atau *client* dari RADIUS *server* dan *gateway*. Untuk dapat berkomunikasi dengan RADIUS server, Chillispot harus dikonfigurasikan mengarah ke alamat IP RADIUS server dan menggunakan *shared secret* yang sama dengan RADIUS.

Edit /etc/chilli.conf. Ubah baris berikut :

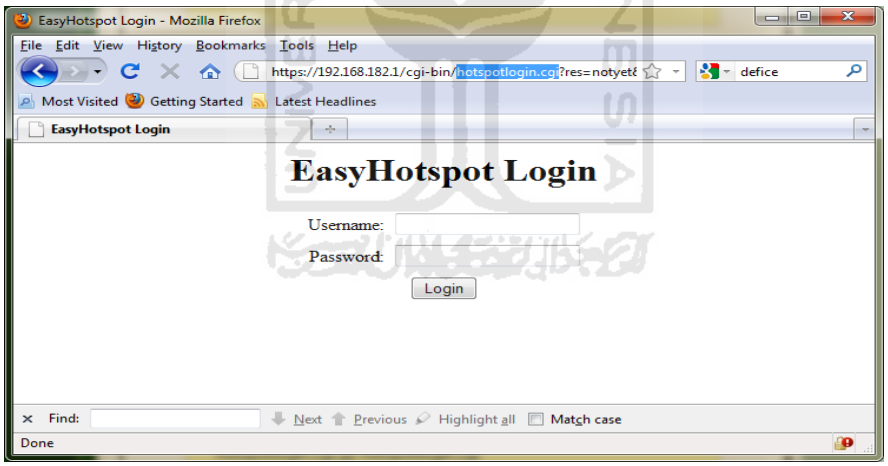
```
radiussecret easyhotspot
radiusserver1 192.168.0.1
radiusserver2 192.168.0.1
```

Chillispot membuat *virtual interface* tun0 yang secara *default* telah diberikan alamat IP 192.168.182.1 dan mengontrol eth1 sebagai DHCP *broadcastinterface* yang menuju jaringan *wireless*(*accesspoint*). Dengan demikian *device* yang terhubung ke *access point* memperoleh IP secara otomatis.

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.182.1  P-t-P:192.168.182.1  Mask:255.255.255.0
          UP POINTOPOINT RUNNING  MTU:1500  Metric:1
          RX packets:1956 errors:0 dropped:0 overruns:0 frame:0
          TX packets:841 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:209021 (209.0 KB)  TX bytes:367772 (367.7 KB)
```

Gambar 4.8 Virtual Interface tun0

Chillispot menggunakan UAM(*Universal Access Method*) untuk melakukan autentikasi. UAM merupakan metode autentikasi yang biasa digunakan pada jaringan *wireless* dengan metode *captive portal. Uamserver* mengacu pada file hotspotlogin.cgi dalam web server. File tersebut memuat form login yang ditampilkan oleh web browser dalam proses autentikasi user RADIUS. *Uamsercret* yang ada di hotspotlogin.cgi harus sama dengan *radiussecret* pada chilli.conf dan *secret* pada clients.conf.



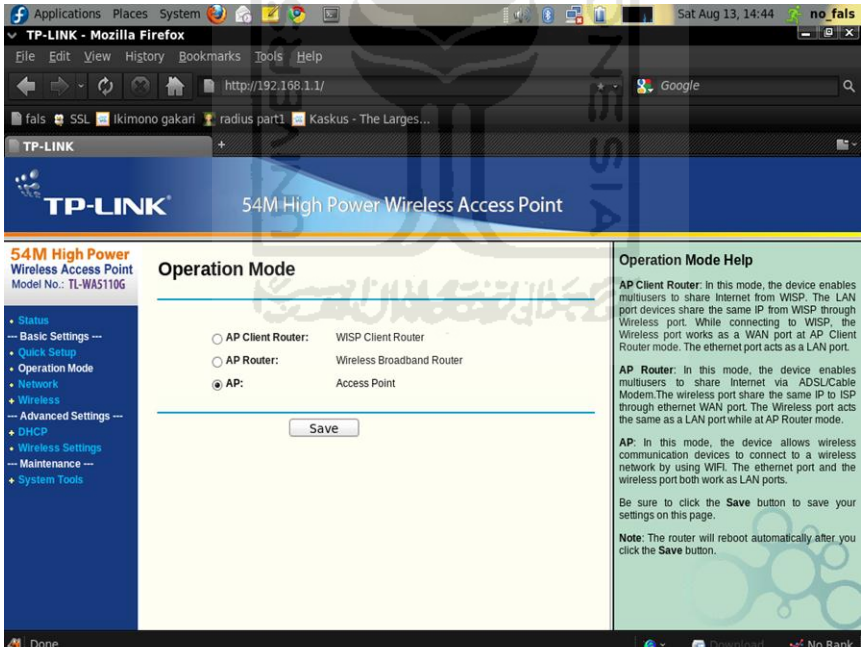
Gambar 4.9 Form Login hotspotlogin.cgi

4.1.4 Instalasi Acces Point

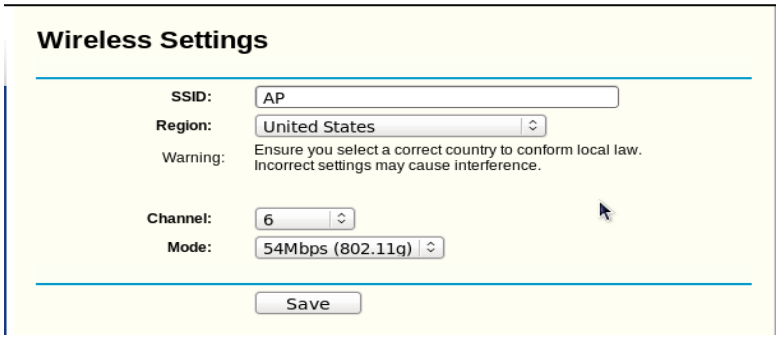
Acces point yang digunakan adalah TP-LINK TL-WA5110G.

Gambar 4.10TP-LINK TL-WA5110G

Dalam kasus ini *Acces point* difungsikan sebagai *bridge*. Fungsi *Wirelessrouter*, DHCP dan fasilitas keamanannya harus di-*disable* karena semua telah ditangani oleh Chillispot. Konfigurasi yang perlu dilakukan adalah set mode sebagai *acces point* dan *broadcast* SSID.



Gambar 4.11 Operation Mode access point



Gambar 4.12 Set SSID

4.2 Pengujian

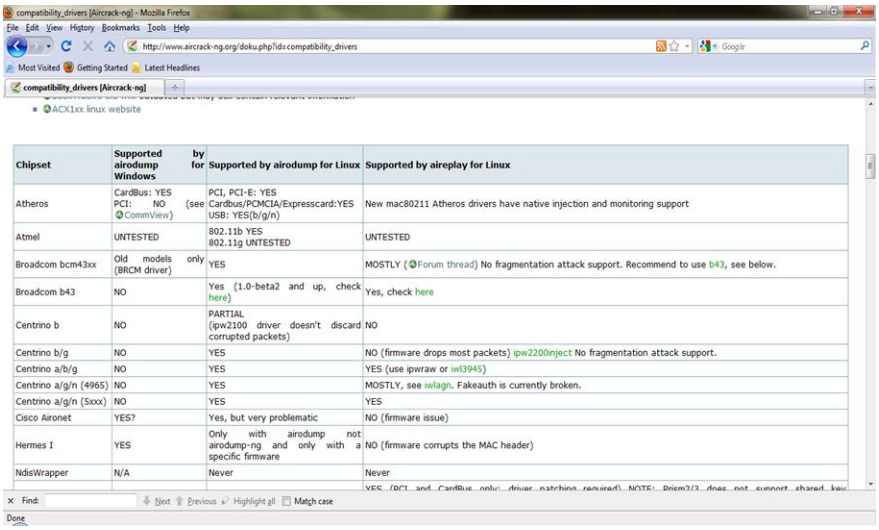
Tahap – tahap pengujian yang dilakukan adalah sebagai berikut :

4.2.1 Sniffing Jaringan Wireless

Jaringan *wireless* menggunakan sinyal radio sebagai media transmisinya. Metode transmisi ini mempunyai *risk* yang lebih besar dari pada jaringan *wired*. Paket data yang ditransmisikan mudah ditangkap oleh *intruder* karena sifat sinyal yang menyebar.

Teknik yang digunakan adalah *passive sniffing*. Untuk melakukan *passive sniffing* di jaringan *wireless*, WLAN card yang digunakan sebagai *sniffer* tidak perlu terhubung ke jaringan. Yang harus dilakukan adalah membuat WLAN card dapat menangkap paket – paket data yang bertaburan.

Agar dapat mengkap semua paket di jaringan wireless, WLAN card harus diset menjadi *promiscuous/monitor mode*. Tidak semua WLAN card mendukung *promiscuous mode*. Keterangan tentang *chipset* dan *driver* yang memenuhi syarat dapat di lihat di http://www.aircrack-ng.org/doku.php?id=compatibility_drivers



Chipset	Supported by airodump for Windows	Supported by airodump for Linux	Supported by aireplay for Linux
Atheros	CardBus: YES PCI: NO (see CommView)	PCI, PCI-E: YES Cardbus/PCMCIA/Expresscard:YES USB: YES(b/g/n)	New mac80211 Atheros drivers have native injection and monitoring support
Atmel	UNTESTED	802.11b YES 802.11g UNTESTED	UNTESTED
Broadcom bcm43xx	Old models only (BRCM driver)	YES	MOSTLY (Forum thread) No fragmentation attack support. Recommend to use b43, see below.
Broadcom b43	NO	Yes (1.0-beta2 and up, check here)	Yes, check here
Centrino b	NO	PARTIAL (ipw2100 driver doesn't discard corrupted packets)	NO
Centrino b/g	NO	YES	NO (firmware drops most packets) ipw2200inject No fragmentation attack support.
Centrino a/b/g	NO	YES	YES (use ipwraw or iwl3945)
Centrino a/g/n (4965)	NO	YES	MOSTLY, see iwlagn. Fakeauth is currently broken.
Centrino a/g/n (5xxx)	NO	YES	YES
Cisco Aironet	YES?	Yes, but very problematic	NO (firmware issue)
Hermes I	YES	Only with airodump not airodump-ng and only with a specific firmware	NO (firmware corrupts the MAC header)
NdisWrapper	N/A	Never	Never

Gambar 4.13 aircrack-ng.org

Tools yang digunakan adalah aircrack-ng. Aircrack-ng adalah kumpulan *tools* yang digunakan untuk melakukan *hacking* terhadap jaringan *wireless.* Tools yang termasuk dalam aircrack-ng adalah airbase-ng, aircrack-ng, airdecap-ng, airdecloak-ng, aireplay-ng, airmon-ng, airodump-ng, airtun-ng dan lain - lain

Langkah pertaman yang dilakukan adalah set WLAN card(wlan0) menjadi *promiscuous/monitor mode.*

```
# airmon-ng start wlan0
```

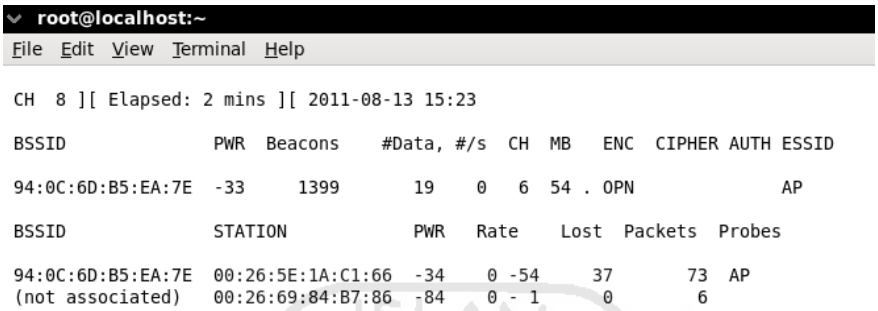
```
File  Edit  View  Terminal  Help
[root@localhost ~]# airmon-ng start wlan0

Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
1405    avahi-daemon
1406    avahi-daemon
1599    NetworkManager
1667    wpa_supplicant

Interface       Chipset         Driver

wlan0           Intel 3945ABG   iwl3945 - [phy0]
                                (monitor mode enabled on mon0)
```

Gambar 4.14 Airmon-ng

terlihat muncul *interface* baru mon0 yang berfungsi menangkap semua paket yang bertebaran di jaringan *wireless*.

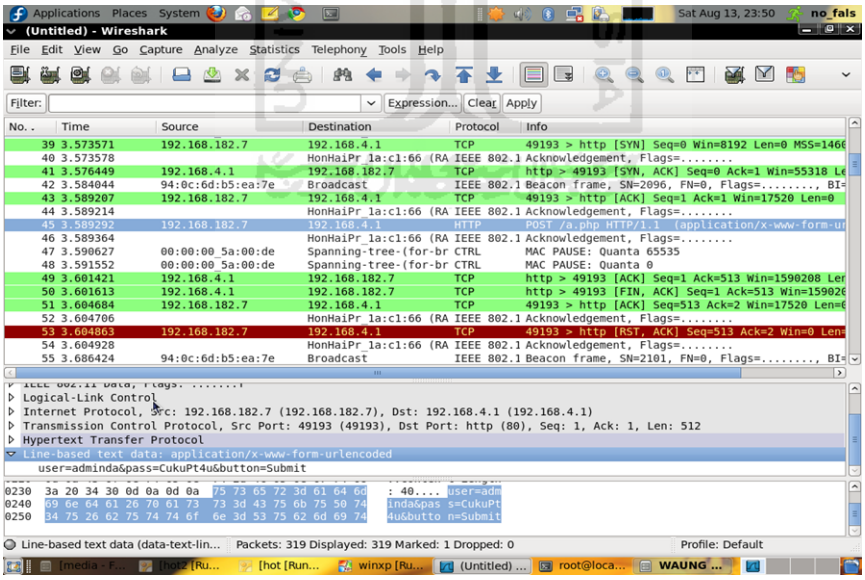
Untuk mengetahui semua SSID, *channel*, MAC *address* yang aktif gunakan airodump.

```
# airodump-ng mon0
```



Gambar 4.15 Capture Airodump-ng

Untuk meng – *capture* dan menganalisa paket data gunakan wireshark. Capture – option pilih *interface* mon0 lalu start



Gambar 4.16 Capture Wireshark

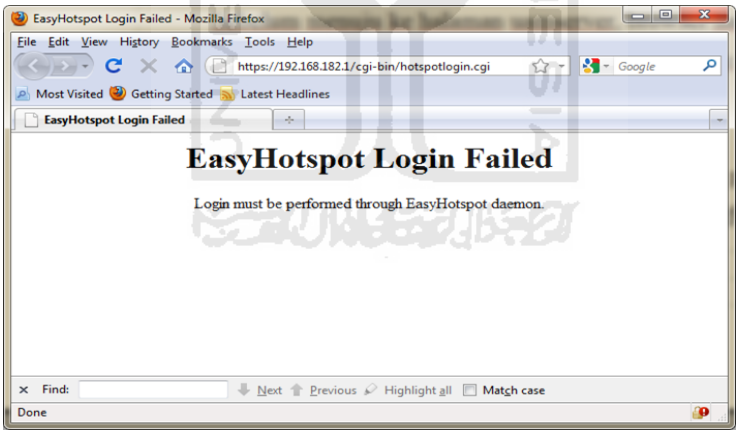
Terlihat bahwa data yang ditransmisikan tidak terenkripsi. Dari celah tersebut kemungkinan bisa didapatkan informasi yang dapat mengusik *privacy,* integritas data dan bahkan dapat menimbulkan ancaman.

Dari hasil pengujian tersebut dapat disimpulkan bahawa sistem RADIUS masih sangat rawan dengan *passive sniffing*karena data yang ditransmisikan melalui WLAN tidak terenkripsi.

4.2.2 Memantau Proses Otentikasi

Clientwireless yang telah terkoneksi ke *access point* mencoba mengakses suatu website lewat browser. Chillispot memaksa *client* tersebut untuk melakukan otentikasi dengan cara me – *redirect* ke http://192.168.182.1:3990 yang merupakan Chillispot web server dan me – *redirect* lagi ke alamat uamserver di https://192.168.182.1/cgi-bin/hotspotlogin.cgi untuk memasukkan *username* dan *password* yang akan diteruskan ke RADIUS *server*.

Sebelum menuju ke halaman *uamserver*, browser harus lebih dahulu melewati port 3990. Jika browser mencoba untuk langsung menuju *uamserver* maka *uamserver* akan memunculkan pesan kesalahan



Gambar 4.17 Easyhotspot Login Failed

Apabila *uamserver* tidak menggunakan *https* maka proses autentikasi akan sangat mudah disadap walaupun hanya dengan *passive sniffing*. Apabila *uamserver* menggunakan *https* maka *sniffer* tidak akan mendapatkan apa yang diinginkannya karena data yang ditransmisikan terenkripsi.

Dari pengujian di atas disimpulkan bahwa sistem RADIUS bisa melakukan enkripsi pada proses *login*/otentikasi akan tetapi tidak lebih dari itu. Data yang

ditransmisikan pada jaringan *wireless*-nya di luar proses *login* tidak terenkripsi.

4.2.3 ARP Spoofing

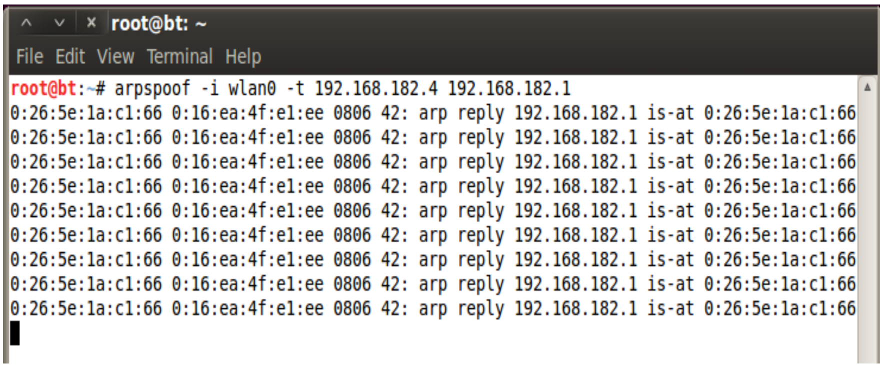
Arp spoofing adalah salah teknik yang digunakan pada *man in the middle attack*. Teknik *arp spoofing* ini sama seperti yang dilakukan oleh *software* netcut. Tujuannya adalah mengelabuhi *client wireless* bahwa *wireless card* milik *attacker* adalah NAS sehingga data yang akan dikirim ke NAS yang asli akan diambil komputer *attacker* setelah itu tinggal kemauan dari penyerang apakah data itu inngin dilihat, diteruskan atau di putus. Cara tersebut dilakukan dengan mengirimkan paket arp pada client wireless. Berikut ini akan dilakukan simulasi arp spoofing pada jaringan *wireless*.

Langkah pertama adalah mencari *IP address* yang aktif sebagai calon korban. Lakukan *scanning* dengan nmap. Range *IP address* yang di – *scan* adalah antara 192.168.182.1 sampai 192.168.182.254.

```
$ nmap 192.168.182.1-254

Starting Nmap 5.51 ( http://nmap.org ) at 2011-09-15 12:03 WIT
Nmap scan report for 192.168.182.3
Host is up (0.031s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3306/tcp open  mysql
MAC Address: 00:1C:BF:6A:A1:69 (Intel Corporate)

Nmap scan report for 192.168.182.4
Host is up (0.033s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:16:EA:4F:E1:EE (Intel)
```

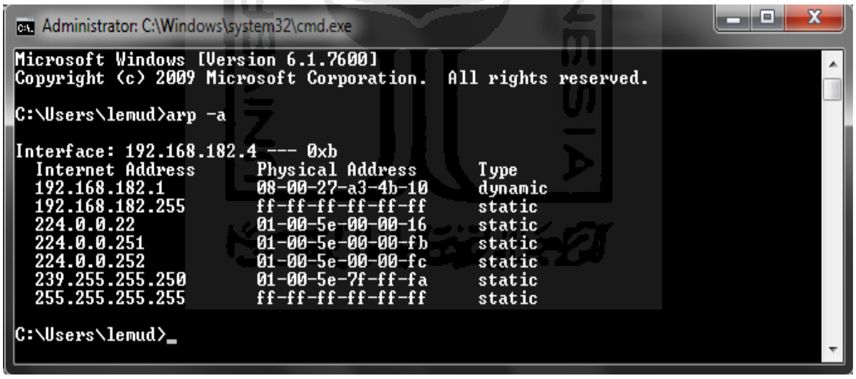
Gambar 4.18 nmap scanning

Misal target serangan adalah *IP address* 192.168.182.4. Setelah itu dilakukan *arp spoofing* ke target 192.168.182.4. Tujuannya memberikan informasi ke 192.168.182.4 bahwa 192.168.182.1(*gateway*) sekarang berada di *MAC attacker*.

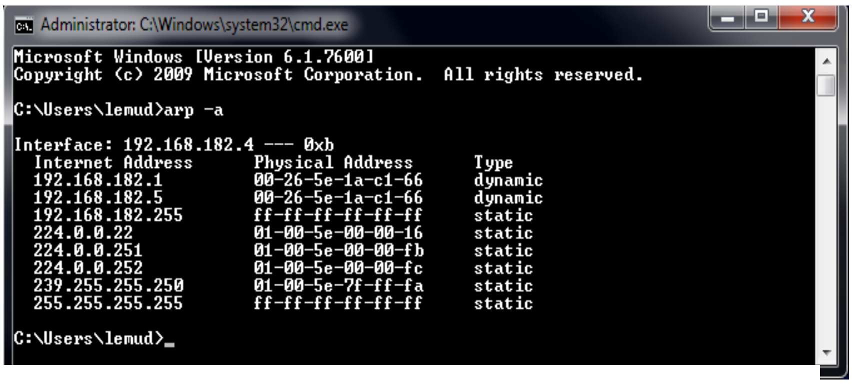


Gambar 4.19 arpspoof

Jika periksa di komputer korban, maka *gateway* sudah berubah terdaftar menjadi MAC milik *attacker*. Periksa arp tabel dengan perintah **arp -a**.



Gambar 4.21 Tabel ARP Sebelum Serangan



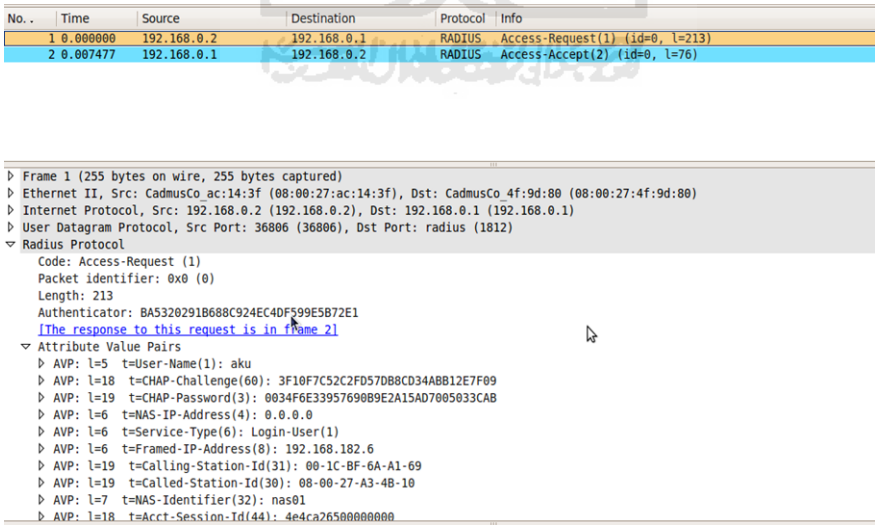
Gambar 4.20 Tabel ARP setelah serangan arpspoof

Chillispot telah dapat mencegah *arpspoofing*. Ketika *attacker* berusaha mem – *forward*paket ke chillispot ternyata tidak berhasil. Yang terjadi adalah korban arp psoofing kehilangan *routing* ke gateway. Hilangnya *routing* ke *gateway* membuat komputer korban tidak bisa mengakses jaringan diluar jaringan chillispot. *Attacker*-pun tidak bisa memonitor *traffic* lebih dalam karena akses yang diminta korban selalu gagal.

Dari pengujian diatas dapat disimpulkan bahwa sistem RADIUS telah dapat mencegah *arpspoofing*akan tetapi masih terdapat kelemahan karena *userwireless* yang terkena *arpspoofing* kehilangan *routing* ke *gateway*. Dengan kata lain user tersebut telah terkena DoS.

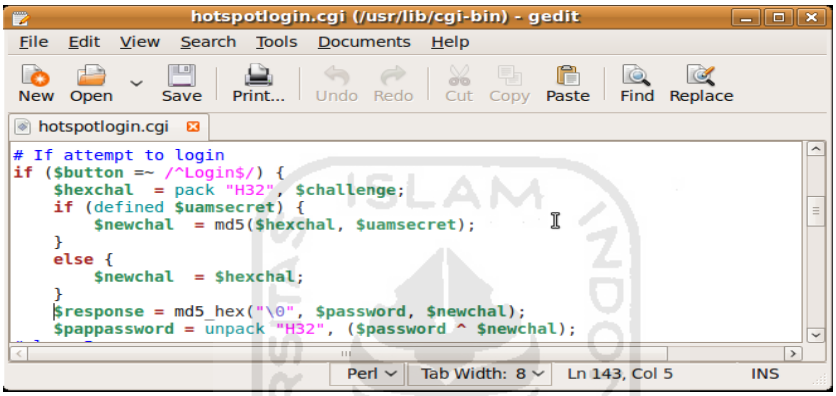
4.2.4 Paket Acces-Request

Ketika *user* melakukan proses *login* pada sistem yang terjadi adalah *user* melakukan *posting* ke uamserver chillispot dan terjadi proses authentikasi. Uamserver meneruskannya dengan mengirim paket access-request ke RADIUS server.



Gambar 4.22 Paket Access-request

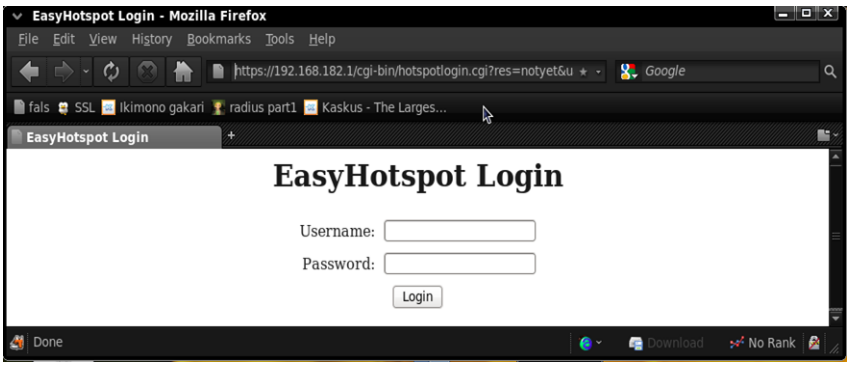
Dalam paket access-request tersebut atribut User-Name dikirim tanpa enkripsi sedangkan *password* dikirimkan sebagai CHAP-Password yang telah dienkripsi. Enkripsi yang dilakukan pada *password* adalah dengan melakukan hash terhadap *password* yang telah digabung dengan karakter "\0" dan *challenge* yang diberikan chillisopot lewat web browser saat form *login* muncul. Berikut ini adalah potongan *script* hotspotlogin.cgi pada web *server* chilllispot yang digunakan untuk membentuk atribut Chap-Password :



Gambar 4.23 Script Pembuatan CHAP-Password

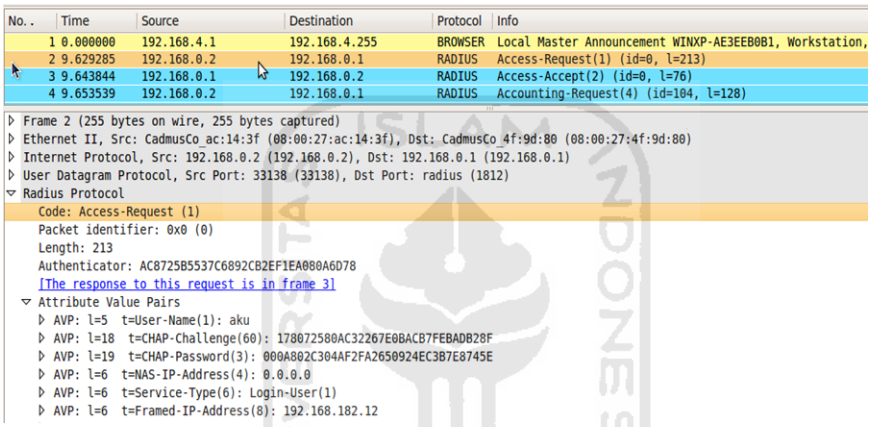
Pada potongan *script* tersebut, variabel $response lah yang digunakan untuk membentuk atribut Chap-Password pada paket Access-Request. Untuk membuktikannya berikut ini akan dilakukan simulasi otentikasi.

Langkah pertama saat *user* berusaha mengakses jaringan luar maka chillispot akan me – *redirect* browser ke halaman*login*. Di halaman tersebutlah *challenge* diberikan pada *user*. *Challenge* tersebut selalu berubah setiap kali *request*.



Gambar 4.24 Pemberian Challenge

Challenge yang diberikan oleh chillispot terletak pada url web browser. https://192.168.182.1/cgi-bin/hotspotlogin.cgi?res=notyet&uamip=192.168.182.1&uamport=3990&challenge=d548307dd2526574163968e3db8d1b0f&nasid=nas01&mac=00-1C-BF-6A-A1-69. Terlihat *challenge* acak yang diberikan oleh chillispot adalah d548307dd2526574163968e3db8d1b0f. Setelah itu user melakukan *login* dengan *username***aku** dan *password***aku**. Chillispot kemudian memprosesnya dan mengirimkan paket Access-Request ke RADIUS server



Gambar 4.25 CHAP-Password

:

Pada paket Access-Request tersebut terlihat attribut Chap-Password yang di –*generate* adalah **000A802C304AF2FA2650924EC3B7E8745E**. Untuk mengetahui proses enkripsi tersebut, berikut ini akan di buat *script* php sederhana untuk mensimulasikan pembentukan atribut Chap-Password. Komponen yang terlibat dalam simulasi ini adalah :

Challenge yang diberikan chillispot lewat web browser :

d548307dd2526574163968e3db8d1b0f.

Uamsecret : **easyhotspot**

Password yang diinputkan user : **aku**

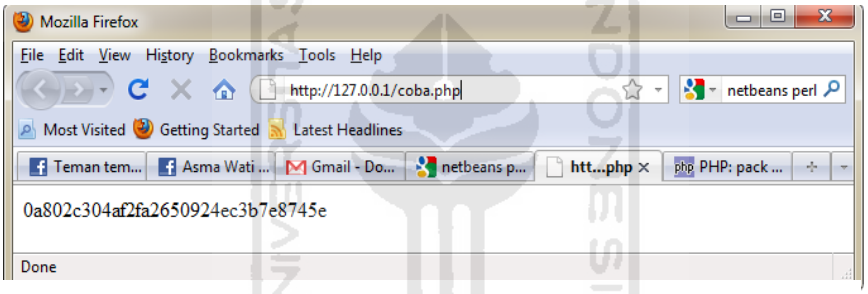
Output merupakan chap-pasword yang berhasil diberntuk

0a802c304af2fa2650924ec3b7e8745e

isi dari scrip php adalah :

```
<?
$challenge = "d548307dd2526574163968e3db8d1b0f";
$uamsecret = "easyhotspot";
$pwd  = "aku";
$hexchal = pack('H32',  $challenge);
$newchal = pack('H*', md5($hexchal.$uamsecret));
$response = md5("\0" . $pwd . $newchal);
echo $response;
?>
```

Jika file php tersebut dieksekusi di *web server* maka akan muncul *output*berupa **0a802c304af2fa2650924ec3b7e8745e**.



Gambar 4.26 Output Hashing dengan PHP

Data *user* yang melakukan *login* tersebut disimpan pada *record* tabel **radpostauth** pada database RADIUS server.

	id	username	pass	reply	authdate
	121	aku	0x006b4d7bbbb766dfcbcbecb13db5eafd39	Access-Accept	2011-08-18 17:48:01
	122	aku	0x00fdfb7c8cf87384a1ebc458e2e7282ffc	Access-Accept	2011-08-18 17:51:1[illegible]
	123	guppot5	0x00d113ab3c1374b94c8492beb0ae220777	Access-Accept	2011-09-10 03:12:48
	124	aku	0x00d9d6e6c08e2765808dad416641545848	Access-Accept	2011-09-15 18:59:22
	125	kamu	0x00f17fc82f1d12592d1781811f553dcb48	Access-Accept	2011-09-15 19:00:39
	126	kamu	0x00dd5a189d22716c75123d598233aa07c2	Access-Accept	2011-09-15 22:30:15
	127	aku	0x0000954b6421c64c7158461ffe549d16f5	Access-Accept	2011-09-15 22:32:09
	128	kamu	0x0089a653026002b57f2b841e266fa71ab1	Access-Accept	2011-09-15 22:51:09
	129	aku	0x002f25e5c702acc3aad6cef6c48225facb	Access-Accept	2011-09-16 01:02:15
	130	aku	0x0056ffa0cb4f1[illegible]451fa43f025726d8ae9f	Access-Accept	2011-09-16 10:35:09
	131	aku	0x000a802c304af2fa2650924ec3b7e8745e	Access-Accept	2011-09-16 10:38:43

Check All / Uncheck All *With selected:*

<< < Show : 30 row(s) starting from record # 0 Page nu

Gambar 4.27 Tabel radpostauth

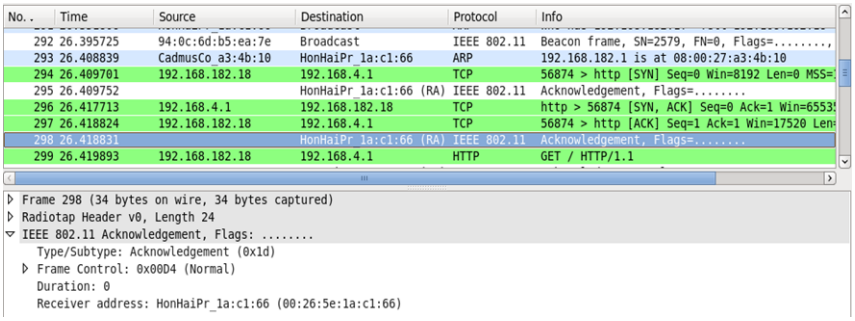
Pada *record* database tersebut terlihat bahwa enkripsi *password* yang dihasilkan berbeda satu sama lain walaupun berasal dari *username* dan *password* yang sama.

Dari simulasi yang telah dilakukan menunjukkan bahwa enkripsi *password* yang digunakan cukup bagus. Walaupun *attacker* dapat menangkap *hash* dari *passworduser*, semua akan menjadi percuma karena nilai *hash* tersebut bukan hanya berasal dari password itu sendiri. Jika *attacker* ingin memecahkannya maka dia harus mengetahui *uamsecret* dan *chaallenge* acak yang diberikan ke *web browser user.*

4.2.5 MAC Address Spoofing

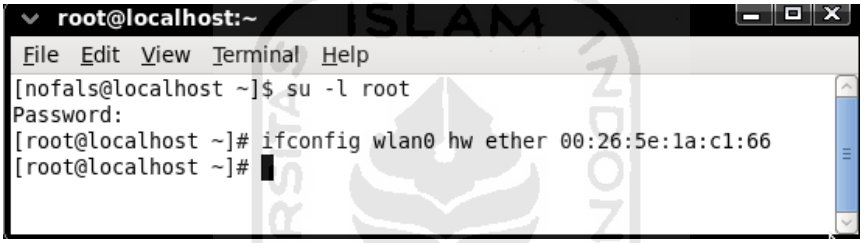
MAC address spoofing adalah tindakan pemalsuan *MAC address*. Teknik ini digunakan untuk melewati proteksi jaringan yang menggunakan autentikasi berbasis *MAC address*. Caranya adalah attacker memalsukan *MAC addressnetwork card* nya dengan *MAC address* milik *user* yang sudah terotentikasi.

Berikut ini akan dilakukan simulasi *MAC address spoofing* untuk melewati proteksi sistem RADIUS pada WLAN. Langkah pertama adalah mencari *authenticated user* yang sedang terkoneksi ke jaringan wireless. Ubah WLAN card ke *promiscuous/monitor mode*. Setelah itu *capture* paket-paket *wireless* dengan wireshark. Ini dilakukan agar *attacker* tidak salah sasaran. karena walaupun belum terautentikasi user yang mencoba melakukan koneksi ke *accesspoint* akan diberi IP address oleh DHCP chillispot. User yang telah terautentikasi biasanya melakukan transfer data dari dan ke jaringan luar chillispot.



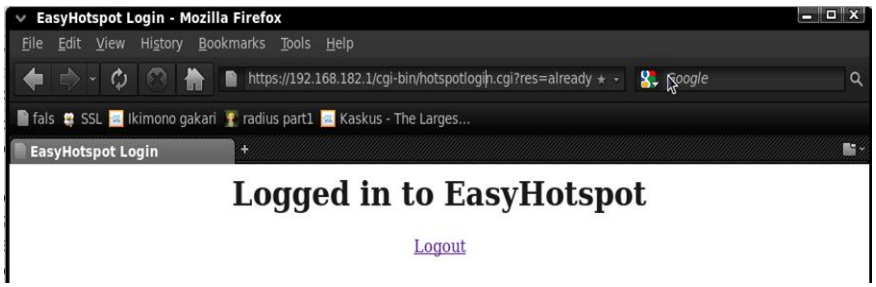
Gambar 4.28 Passive sniffing

Setelah mendapatkan IP address authenticated user, ubahlah MAC address attacker menjadi sama seperti MAC address authenticated user.



Gambar 4.29 MAC Address Spoofing

Up – kan kembali WLAN card lalu minta koneksi ke Access Point. Chillispot akan memberikan *IP address* yang sama seperti *user* yang asli kepada *attacker* dan *user* yang asli kehilangan koneksinya. Sekarang *attacker* sudah sepenuhnya terautentikasi dan bebas memanfaatkan layanan yang diberikan jaringan *wireless*. Ketika *browserattacker* mengakses *webserver* chillispot di http://192.168.182.1:3990, chillispot mengarahkannya ke https://192.168.182.1/cgi-bin/hotspotlogin.cgi?res=already&uamip=192.168.182.1&uamport=3990&nasid=nas01&mac=00-26-5E-1A-C1-66. Hal tersebut menjadi tanda bahwa kini attacker sudah melewati proses otetikasi.



Gambar 4.30 User Telah Login

Dari pengujian tersebut dapat disimpulkan bahwa sistem RADIUS masih lemah terhadap MAC *addressspoofing*. *Attacker* dapat mem – *bypasslogin page* dengan cara memalsukan MAC *addressuser* yang telah terotentikasi.

4.3 Audit sistem RADIUS

Langkah dalam proses audit berikutt dibagi menjadi tiga bagian yaitu audit Access Point, Captive portal dan RADIUS server.

4.3.1 Access Point

Peran *AccessPoint* pada sistem ini sangat penting karena AP berperan sebagai konsentrator dan media bagi user wireless untuk mengakses sistem. Beberapa hal yang perlu diperhatikan adalah:

a. Konfigurasi AP

1. **Apakah AP sudah menggunakan firmware terbaru.**

Dalam firmware terbaru biasanya telah dilakukan perbaikan – perbaikan dari firmware sebelumnya. Sehingga dengan menggunakan firmware terbaru diharapkan dapat meningkatkan efektifitas dan keamanan AP.

2. **Apakah konfigurasi AP sudah diubah dari konfigurasi default.**

Konfigurasi AP terutama IP address dan password default harus diganti. Tindakan tersebut dapat meningkatkan keamnanan sistem, minimal dapat menghambat langkah serangan attacker.

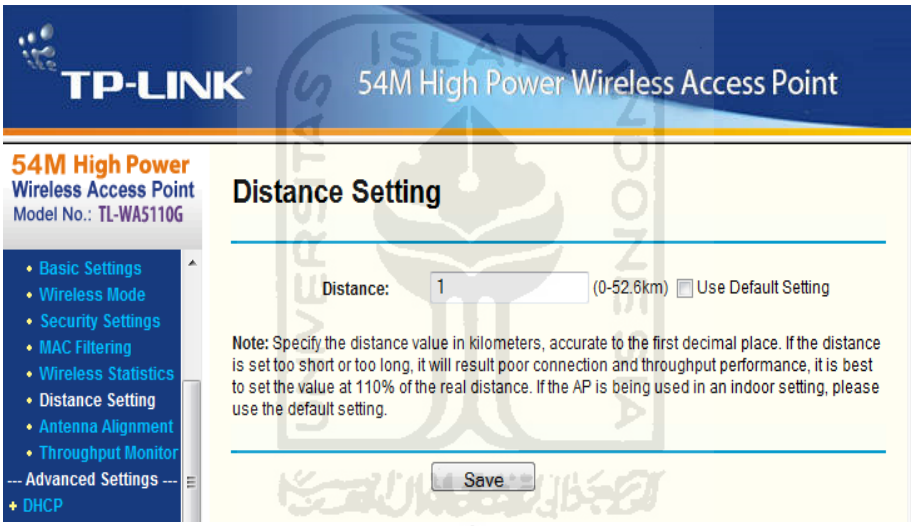
b. Sinyal AP

1. **Pastikan access point tidak menggunakan power yang berlebihan.**

Menggunakan power AP yang berlebihan dapat meningkatkan kekuatan sinyal wireless. Sinyal wireless yang terlalu kuat mengakibatkan jaringan bisa diakses diluar coverage area yang diinginkan.

2. **Apakah coverage area AP sudah sesuai dengan kebutuhan.**

Membatasi *coverage area* sangat penting dalam keamanan jaringan wireless. jika *coverage area* - nya berlebihan dapat memberikan lebih banyak ruang yang memmungkinkan bagi *attacker* untuk melakukan serangan.



Gambar 4.31 Distance setting

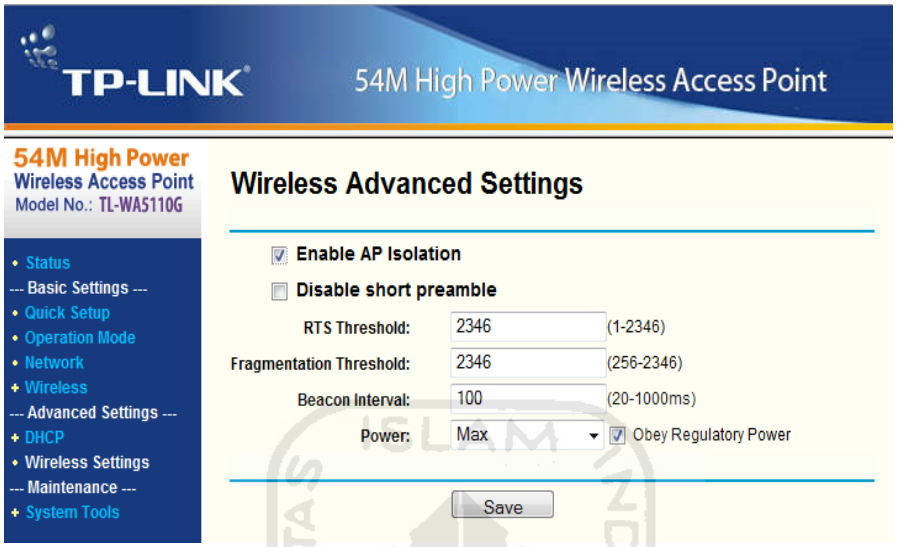
3. **Matikan AP jika tidak digunakan**

Jika AP tidak digunakan dalam waktu cukup lama, lebih aman jika access point dimatikan. Tindakan ini dilakuakn untuk mencegah seseorang melakukan ekplorasi dan mengambil alih AP tersebut.

4. **Jika menggunakan hanya satu buah Ap, apakah sudah menerapkan AP isolation.**

Fitur *repeater* yang sekarang umum terdapat pada AP bahkan AP kelas bawah sekalipun dapat dengan mudah meneruskan sinyal wireless kita. Hal tersebut

dapat mengakibatkan jaringan wireless semakin meluas dan tak terkendali. Dengan mengaktifkan Ap *isolation* dapat mengamankan jaringan wireless dari *fake AP* tersebut.



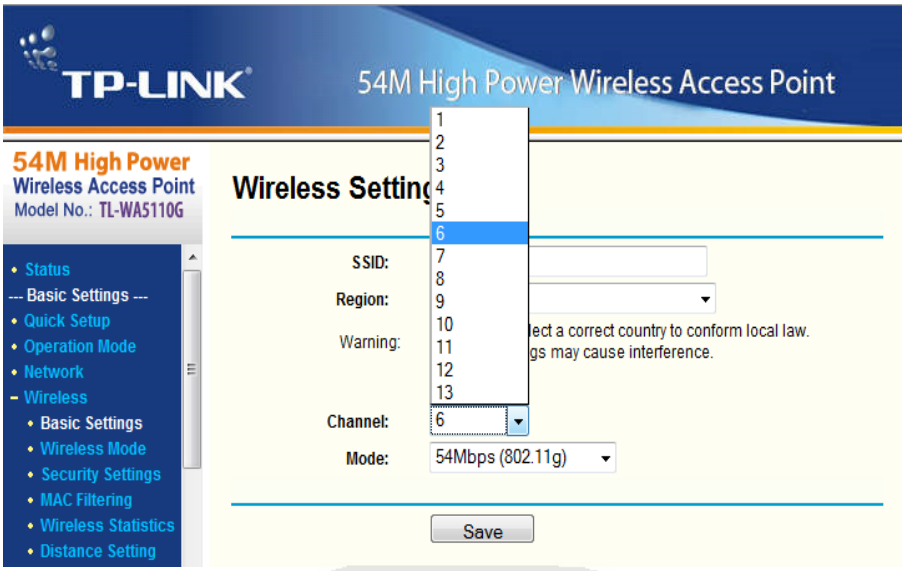
Gambar 4.32 AP isolation

5. **Jika menggunakan lebih dari satu Ap, apakah sudah menggunakan WDS**

Untuk memperluas jaringan wireless, salah satu solusinya adalah dengan menggunakan lebih dari satu AP. Dimana AP yang satu akan me – relay sinyal dari AP sumber. Dalam kasus ini lebih aman jika kita menggunakan metode *Wireless Distributed System*(WDS). Dengan metode WDS, AP yang satu dengan AP sumber dengan AP yang lain akan saling terotentikasi sehingga akan meminimalkan serangan *fake AP* atau *rouge AP*.

6. **Apakah sudah menggunakan channel yang lapang.**

Menggunakan *channel* yang padat dapat mengakibatkan *jamming* yang tidak disengaja karena adanya interferensi dari *wireless device* lain yang menggunakan frekuensi yang sama. sinyal - sinyal tersebut mengakibatkan *noise* yang dapat menggangu komunikasi antara AP dan *user wireless*. Oleh karena itu pemilihan *channel* sangat penting untuk menjaga kualitas jaringan *wireless*.



Gambar 4.33 Channel

7. Apakah administrator sudah melakuakn sniff pada jaringan wireless.

Sangat penting bagi administrator untuk melakukan *sniffing* pada jaringan wirelessnya. Dengan *sniffing* atau *monitoring* jaringan *wireless*, admin dapat mengetahui kegiatan yang dilakukan oleh *user wireless* dan dapat mendeteksi masalah ataupun serangan yang muncul.

8. Lakukan pengecekan terhadap kemungkinan keberadaan rouge AP

Pastikan tidak ada *rouge* AP yang terkoneksi ke jaringan wireless. Rouge AP sangat berbahaya karena dapat memperluas area wireless, pengaksesan jaringan secara ilegal dan penurunan kualitas jaringan.

4.3.2 Captive Portal

1. Apakah portal sudah menggunakan https.

Portal yang terletak di web server harus menggunakan https. Karena dari portal itulah user melakukan otentikasi sehingga data user yang ditransmisikan melalui jaringan *wireless* menjadi terenkripsi.

2. Apakah captive portal sudah dapat menangani tipe serangan MITM.

Walaupun belum sepenuhnya dapat menangani tipe serangan MITM, minimal captive portal sudah dapat menanganinya pada level *gateway*. Sehingga ketika terjadi serangan seperti *arp poisioning*, hubungan antara *gateway*, *attacker* dan korban menjadi terputus dan data - data *user* tidak dapat dicuri.

4.3.3 RADIUS Server

1. Aapakah sudah menggunakan shared secret yang baik.

Shared secret diperlukan agar antara RADIUS server dan RADIUS clien(NAS) dapat saling berkomunikasi. Oleh karena itu *shared secret* yang digunakan harus cukup kuat.

2. Apakah Sudah mengubah konfigurasi dan akun default.

Konfifigurasi dan terutama akun *default* harus dirubah. Karena jika tidak dirubah dapat dimanfaatkan oleh attacker.

4.3.4 Checklist

1. Apakah AP sudah menggunakan firmware terbaru.
2. Apakah konfigurasi AP sudah diubah dari konfigurasi default.
3. Pastikan access point tidak menggunakan power yang berlebihan.
4. Apakah coverage area AP sudah sesuai dengan kebutuhan.
5. Matikan AP jika tidak digunakan.
6. Jika menggunakan hanya satu buah AP, apakah sudah menerapkan AP isolation.
7. Jika menggunakan lebih dari satu AP, apakah sudah menggunakan WDS.
8. Apakah sudah menggunakan channel yang lapang.
9. Apakah administrator sudah melakuakn sniff pada jaringan wireless.
10. Lakukan pengecekan terhadap kemungkinan keberadaan rouge AP.
11. Apakah portal sudah menggunakan https.

12. Apakah captive portal sudah dapat menangani tipe serangan MITM.
13. Aapakah sudah menggunakan shared secret yang baik.
14. Apakah Sudah mengubah konfigurasi dan akun default.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil implementasi RADIUS pada WLAN dalam hal keamanan, maka dapat ditarik kesimpulan sebagai berikut :

a. Sistem RADIUS masih sangat rawan dengan *passive sniffing*karena data yang ditransmisikan melalui WLAN tidak terenkripsi.
b. Jaringan wireless berbasis RADIUS dan captive portal telah dapat mencegah *man in the middle attack* pada *gateway*. Akan tetapi masih terdapat celah pada level *user* di bawah *gateway*. Sehingga user yang menjadi terget serangan akan terkena DOS.
c. Enkripsi yang diterapkan cukup baik. Tetapi enkripsi hanya dijalankan pada proses otentikasi saja, sehingga masih sangat rentan terhadap *passive sniffing*.
d. Protokol RADIUS hanya melakukan enkripsi pada *password* saja sedangkan atribut yang lain tidak terenkripsi.
e. Otentikasi masih dapat di bypass dengan MAC *spoofing* dan tidak ada MAC *conflict*.

5.2 Saran

Berdasarkan kekurangan pada implementasi sistem RADIUS, maka berikut ini adalah saran yang semoga berguna dan dapat diterapkan guna meningkatkan keamanan pada jaringan wireless :

a. Gunakan secret yang baik. Panjang secret tidak boleh kurang dari 8 karakter dan merupakan kombinasi huruf besar, huruf kecil, anka dan simbol. Karena pada dasarnya md5 merupakan one way hashing dan hanya bisa di *reverse* dengan *dictionary* dan brute force attack. Dengan secret yang panjang dan acak akan lebih lama bagi attacker untuk

memecahkannya.

b. Diharapkan di masa mendatang penelitian mengenai protokol RADIUS lebih lengkap dengan meneliti semua jenis paket RADIUS.
c. Untuk menambah keamanan jaringan wireless akan lebih baik jika menggunakan WPA2 Enterprise yang merupakan kolaborasi antara WPA2 dan RADIUS server.

DAFTAR PUSTAKA

Setiawan, M.A, & Febyatmoko, G.S. 2006. Sistem Autentikasi, Otorisasi, dan Pelaporan Koneksi User pada Jaringan Wireless Menggunakan Chillispot dan Server Radius. Makalah disampaikan pada Seminar Nasional Aplikasi Teknologi Informasi. Fakultas Teknonologi Industri UII. yogyakarta, 17 Juni.

Setiawan. 2004. *Analisis Keamanan Jaringan Internet menggunakan Hping, Nmap, Nesuss dan Ethereal*. Bandung:Fakultas Teknologi Industri Institut Teknologi Bandung.

Stall, R. 2002. Auditing a Cisco Aironet Wireless Network From an Auditors Perspective. Available at http://it-audit.sans.org/community/papers/auditing-cisco-aironet-wireless-network-auditors-perspective_77.

Rigney, C., Willens, S., Rubens, A., & Simpson, W. 2000. RFC 2865. Remote Authentication Dial In User Service (RADIUS). IETF. Available at http://www.ietf.org/rfc/rfc2865.txt.

Easyhotspot Documentation. Available at http://easyhotspot.inov.asia/index.php/documentation. Diakses pada September 2011.