PRAKTIKUM 6

Wireless Security (WEP,WPA dan Radius)

A. TUJUAN PEMBELAJARAN

1. Mahasiswa mampu memahami cara melakukan keamanan pada jaringan wireless
2. Mahasiswa mampun mengimplementasikan sistem keamanan WEP/WPA/Radius pada jaringan wireless
3. Mahasiswa mampu membangun radius server sebagai pengamanan jaringan wireless.

B. DASAR TEORI

WEP Wired Equivalent Privacy (WEP) adalah algoritma ditinggalkan untuk mengamankan jaringan nirkabel IEEE 802.11. Jaringan nirkabel menggunakan radio menyiarkan pesan dan dengan demikian lebih rentan terhadap penyadapan daripada jaringan kabel. Ketika diperkenalkan pada tahun 1997, WEP dimaksudkan untuk memberikan kerahasiaan sebanding dengan jaringan kabel tradisional.Awal tahun 2001, beberapa kelemahan serius diidentifikasi oleh cryptanalysts dengan hasil bahwa hari ini koneksi WEP dapat retak dengan perangkat lunak tersedia dalam beberapa menit. Dalam beberapa bulan IEEE menciptakan sebuah gugus tugas baru 802.11i untuk melawan masalah. Pada tahun 2003, Wi-Fi Alliance mengumumkan bahwa WEP telah digantikan oleh Wi-Fi Protected Access (WPA).

WPA, WPA2 dan WPA-PSK

WPA (bahasa Inggris: Wi-Fi Protected Access) adalah suatu sistem yang juga dapat diterapkan untuk mengamankan jaringan nirkabel. Metoda pengamanan dengan WPA ini diciptakan untuk melengkapi dari sistem yamg sebelumnya, yaitu WEP. Para peneliti menemukan banyak celah dan kelemahan pada infrastruktur nirkabel yang menggunakan metoda pengamanan WEP. Sebagai pengganti dari sistem WEP, WPA mengimplementasikan layer dari IEEE, yaitu layer

802.11i. Nantinya WPA akan lebih banyak digunakan pada implementasi keamanan jaringan nirkabel. WPA didesain dan digunakan dengan alat tambahan lainnya, yaitu sebuah komputer pribadi (PC).Fungsi dari komputer pribadi ini kemudian dikenal dengan istilah authentication server, yang memberikan key yang berbeda kepada masing-masing pengguna/client dari suatu jaringan nirkabel yang menggunakan akses point sebagai media sentral komunikasi. Seperti dengan jaringan WEP, metoda enkripsi dari WPA ini juga menggunakan algoritma RC4.Pengamanan jaringan nirkabel dengan metoda WPA ini, dapat ditandai dengan minimal ada tiga pilihan yang harus diisi administrator jaringan agar jaringan dapat beroperasi pada mode WPA ini. Ketiga menu yang harus diisi tersebut adalah: * Server o Komputer server yang dituju oleh akses point yang akan memberi otontikasi kepada client. beberapa perangkat lunak yang biasa digunakan antara lain freeRADIUS, openRADIUS dan lain-lain. * Port o Nomor port yang digunakan adalah 1812. * Shared Secret o Shared Secret adalah kunci yang akan dibagikan ke komputer dan juga kepada client secara transparant.Setelah komputer diinstall perangkat lunak otontikasi seperti freeRADIUS, maka sertifikat yang dari server akan dibagikan kepada client.Untuk menggunakan Radius server bisa juga dengan tanpa menginstall perangkat lunak di sisi komputer client. Cara yang di gunakan adalah Web Authentication dimana User akan diarahkan ke halaman Login terlebih dahulu sebelum bisa menggunakan Jaringan Wireless. Dan Server yang menangani autentikasi adalah Radius server.

WPA-PSK

WPA-PSK (Wi-Fi Protected Access – Pre Shared Key) adalah pengamanan jaringan nirkabel dengan menggunakan metoda WPA-PSK jika tidak ada authentikasi server yang digunakan. Dengan demikian access point dapat dijalankan dengan mode WPA tanpa menggunakan bantuan komputer lain sebagai server. Cara mengkonfigurasikannya juga cukup sederhana. Perlu diketahui bahwa tidak semua access point akan mempunyai fasilitas yang sama dan tidak semua access point menggunakan cara yang sama dalam mendapatkan Shared-Key yang akan dibagikan ke client.Pada access point Dlink DWL-2000AP, pemberian Shared-Key dilakukan secara manual tanpa mengetahui algoritma apa yang digunakan. Keadaan ini berbanding terbalik dengan akses point Linksys WRT54G, dimana administrator dapat memilih dari dua algoritma WPA yang disediakan, yang terdiri dari algoritma TKIP atau algoritma AES.Setelah Shared-Key didapat, maka client yang akan bergabung dengan access point cukup memasukkan angka/kode

yang diijinkan dan dikenal oleh access point. Prinsip kerja yang digunakan WPA-PSK sangat mirip dengan pengamanan jaringan nirkabel dengan menggunakan metoda Shared-Key.

WPA2

WPA2 adalah sertifikasi produk yang tersedia melalui Wi-Fi Alliance. WPA2 Sertifikasi hanya menyatakan bahwa peralatan nirkabel yang kompatibel dengan standar IEEE 802.11i. WPA2 sertifikasi produk yang secara resmi menggantikan wired equivalent privacy (WEP) dan fitur keamanan lain yang asli standar IEEE 802.11. WPA2 tujuan dari sertifikasi adalah untuk mendukung wajib tambahan fitur keamanan standar IEEE 802.11i yang tidak sudah termasuk untuk produk-produk yang mendukung WPA.Update WPA2/WPS IE yang mendukung WPA2 fitur berikut:* WPA2 Enterprise IEEE 802.1X menggunakan otentikasi dan WPA2 Personal menggunakan tombol preshared (PSK).* The Advanced Encryption Standard (AES) dengan menggunakan Mode Kontra-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP) yang menyediakan kerahasiaan data, asal data otentikasi, dan integritas data untuk frame nirkabel.* Opsional penggunaan Berpasangan Master Key (PMK) PMK oportunistik cache dan cache. Dalam PMK caching, klien nirkabel dan titik akses nirkabel cache hasil 802.1X autentikasi. Oleh karena itu, akses jauh lebih cepat ketika klien nirkabel menjelajah kembali ke titik akses nirkabel ke klien yang sudah dikonfirmasi.* Opsional penggunaan preauthentication. Dalam preauthentication, WPA2 wireless client yang dapat melakukan otentikasi 802.1X dengan titik akses nirkabel lainnya dalam jangkauan ketika masih terhubung ke titik akses nirkabel saat ini.Anda harus menggunakan IE WPA2/WPS Update bersama-sama dengan berikut:* Wireless access point yang mendukung WPA2.Jaringan Wireless adaptor yang mendukung WPA2.* Windows XP driver adaptor jaringan nirkabel yang mendukung kemampuan berlalunya WPA2 ke Windows Wireless Auto Konfigurasi.Update IE yang WPA2/WPS memodifikasi kotak dialog berikut:* Jika Anda tersambung ke jaringan nirkabel yang mampu WPA2, jenis jaringan yang ditampilkan sebagai WPA2 di Wireless Network Pilih Sebuah kotak dialog.* Pada tab Asosiasi untuk properti dari jaringan nirkabel, daftar Otentikasi Jaringan memiliki opsi tambahan berikut:o WPA2 - untuk WPA2 Enterprise WPA2-PSK - untuk WPA2 Personal

C. TUGAS PENDAHULUAN

Jelaskan kelemahan-kelemahan yang ada pada sistem keamanan jaringan wireless dengan menggunakan WEP.

D. PERCOBAAN

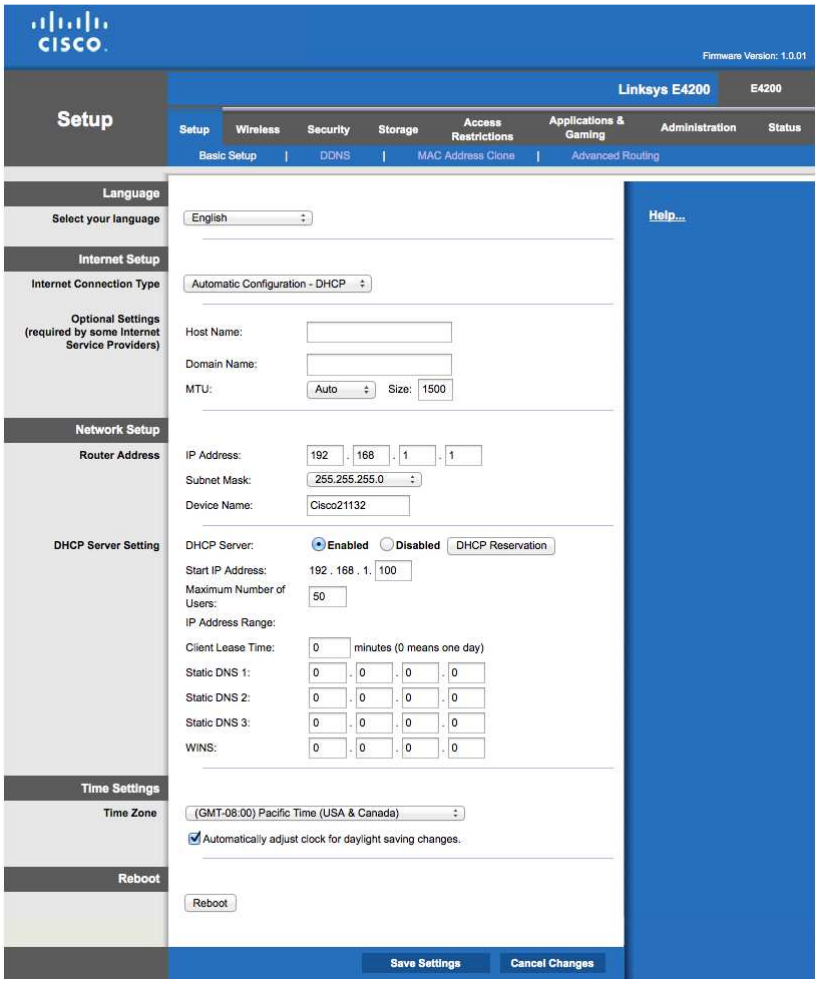
Pada percobaan praktikum ini, perangkat wireless yang digunkanan adalah Wireless Router dengan merk LinkSys E4200.



LinkSys E4200

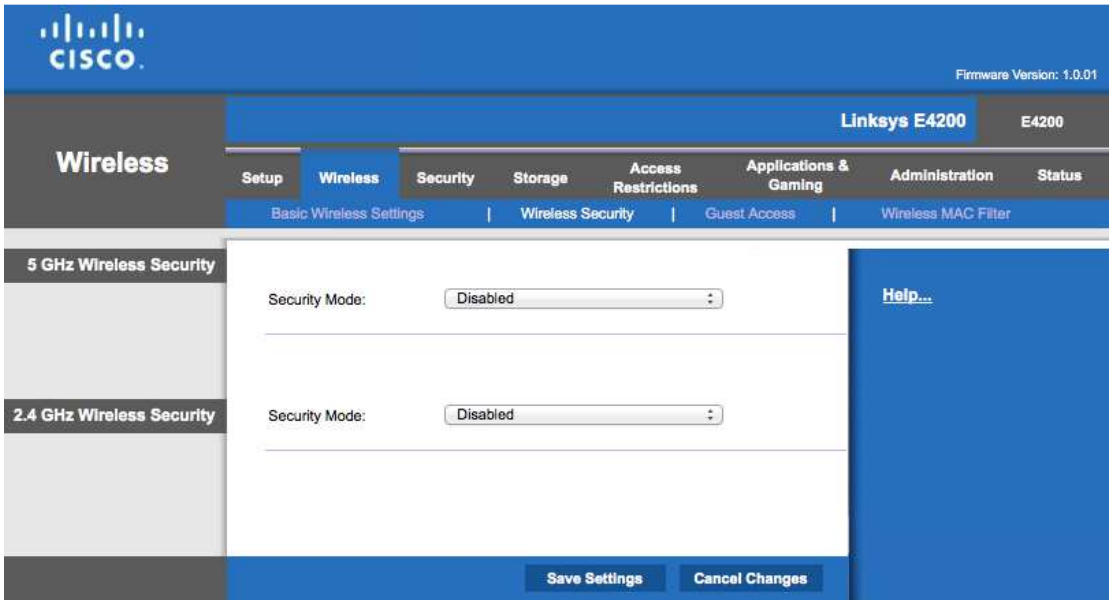
D.1. WEP

1. Terlebih dahulu nyalakan perangkat dengan menghubungkan adaptor dengan perangkat Linksys.
2. Hubungkan kabel UTP dari perangkat Linksys pada port **Ethernet** ke komputer. Dan jangan lupa komputer disetting secara DHCP/Automatic agar mendapatkan IP address dari perangkat Linksys.
3. Akses perangkat Linksys dengan menggunakan browser dengan mengetikkan alamat http://192.168.1.1. Jika diminta password masukkan user: admin, password: admin (setting default dari Linksys). Maka akan tampil halaman management dari Linksys seperti tampak berikut ini:



Web management Linksys

4. Pilih/Klik menu **Wireless → Wireless Security**



Menu wireless security

5. Pada sub menu wireless security terdapat 2 **Security Mode** yaitu untuk radio 5GHz dan 2.4GHz. Dimana pada pada versi Linksys E4200 memiliki 2 radio yang terpasang pada perangkat yang sama. Pada praktikum ini yang akan digunakan hanya pada radio dengan frekuensi 2.4GHz saja.
6. Pilih **Security Mode** untuk **WEP.** Kemudian buka candela terminal pada komputer dengan sistem operasi linux dan ketikkan:

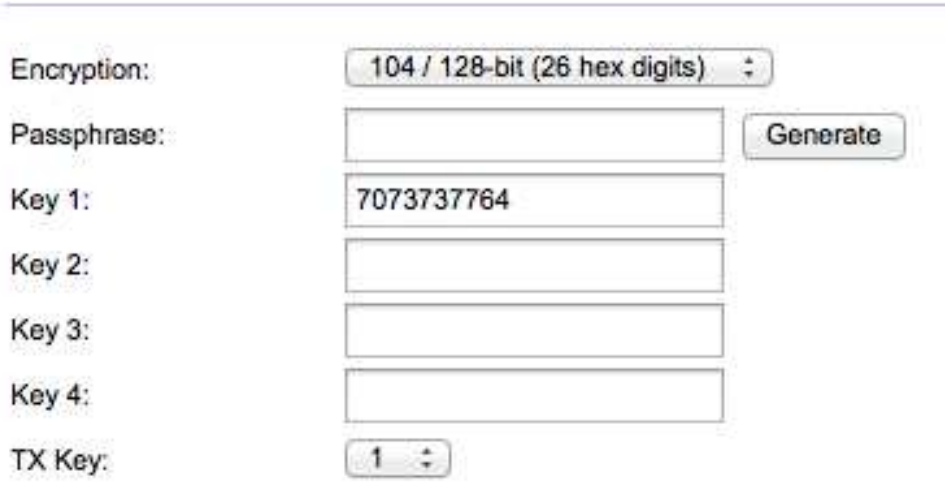
```
idris@debian:~$ echo psswd|hexdump –C
00000000  70 73 73 77 64 0a                        |psswd.|
00000006
```

Dari format diatas **psswd** adalah kata kunci yang akan di konversi menjadi bilangan hex karena LinkSys hanya bisa menggunakan bilangan hex.

Catatan:

Kata kunci yang dapat dimasukkan untuk WEP adalah memiliki panjang max 10 hex digit (5 karakter ASCII) atau 26 hex digit.

7. Maka dari perintah diatas bilangan hex yang akan dimasukkan adalah ***7073737764***



Form entry key WEP

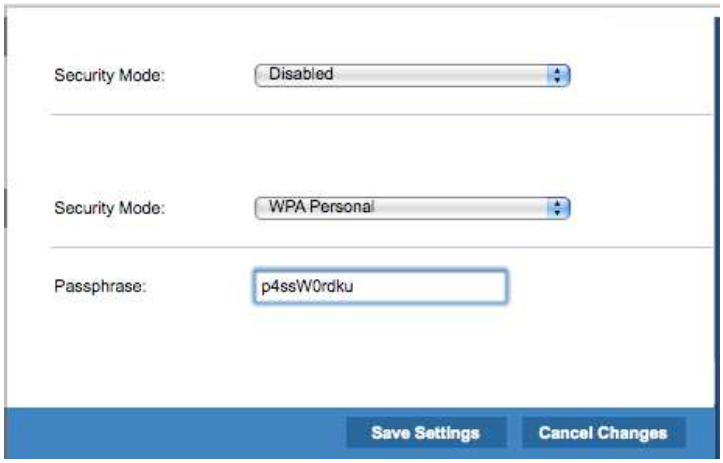
8. Klik tombol “Save Setting” dan ujicobakan pada perangkat wireless client.

D.2. WPA

Sistem keamanan wireless dengan menggunakan WPA dibagi menjadi 2 macam yaitu **personal** dan **enterprise.**

Untuk yang berjenis enterprise WPA akan melibatkan radius server yang akan dibahas pada percobaan ke 3 dibagian **radius**, sedang personal langkah-langkahnya adalah sebagai berikut:

1. Lakukan langkah 1 s/d 5 seperti pada **percobaan I**
2. Pilih **Security Mode** untuk **WPA Personal.** Kemudian masukkan Passphrase-nya misalkan: ***p4ssW0rdku***



Form entry passphrase WPA

3. Klik tombol “Save Setting” dan ujicobakan pada perangkat wireless client.

D.3.RADIUS

Pertama kita persiapkan terlebih dahulu server untuk radiusnya, kemudian dilanjutkan dengan setting radius pada wireless router Linksys. Berikut langkah-langkah untuk membuat radius servernya dilanjutkan dengan setting pada wireless router Linksys:

1. Sebelum melakukan percobaan hendaklah melakukan pengecekan terhadap sistem operasi yang anda gunakan:

```
root@debian:~# cat /etc/debian_version
6.0.5
```

2. Lakukan installasi daemon radius

```
root@debian:/home/idris# apt-get install freeradius
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  freeradius-common freeradius-utils libdbi-perl libfreeradius2 libltdl7 libnet-daemon-perl libperl5.10 libplrpc-perl libpython2.6 ssl-cert
Suggested packages:
  freeradius-ldap freeradius-postgresql freeradius-mysql freeradius-krb5 openssl-blacklist
The following NEW packages will be installed:
  freeradius freeradius-common freeradius-utils libdbi-perl libfreeradius2 libltdl7 libnet-daemon-perl libperl5.10 libplrpc-perl libpython2.6 ssl-cert
0 upgraded, 11 newly installed, 0 to remove and 0 not upgraded.
Need to get 3,957 kB of archives.
After this operation, 11.1 MB of additional disk space will be used.
```

3. Tambahkan client untuk network dari wireless router dengan mengedit file *client.conf*

```
root@debian:~# vim /etc/freeradius/clients.conf
```

Tambahkan script berikut pada baris paling bawah sendiri:

client 10.252.108.0/16 {

secret = kunciku

shortname = network-wireless-ku

}

4. Lakukan penambahan user pada radius

```
root@debian:~# vim /etc/freeradius/users
```

Tambahkan script berikut pada baris paling bawah sendiri:

idris Cleartext-Password := "eepis"

dimana dari script tersebut menunjukkan usernya adalah **idris** dan password adalah **eepis**

5. Restart daemon radius server

```
root@debian:~# /etc/init.d/freeradius restart
Stopping FreeRADIUS daemon: freeradius.
Starting FreeRADIUS daemon: freeradius.
```

6. Ujicoba atau test radius servernya

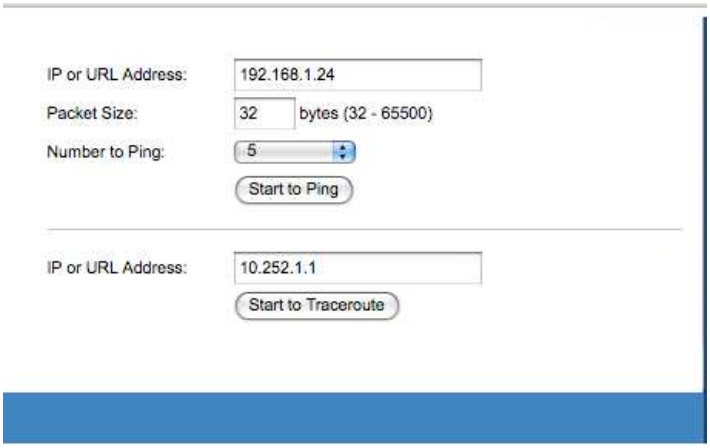
```
root@debian:~# radtest idris eepis localhost 1812 kunciku
Sending Access-Request of id 128 to 127.0.0.1 port 1812
        User-Name = "idris"
        User-Password = "eepis"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 1812
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=128, length=20
```

Dari perintah tersebut diatas dapat dijelaskan dengan syntax sebagai berikut:

Radtest <username> <password> <server radius> <nas-port-number> <secret key>

Untuk *nas-port-number* secara default adalah 1812 sedangkan *secret-key* defaultnya adalah testing123, jika ingin merubah *secret-key* dapat mengedit file *client.conf*

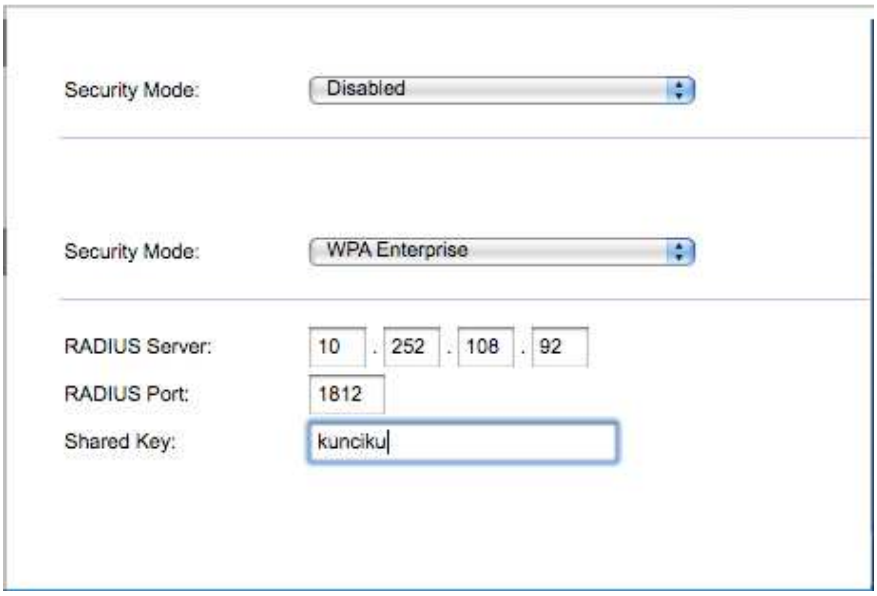
4. Pastikan wireless router bisa berkomunikasi dengan server radius dengan menggunakan menu **Administratrion → Diagnostics**



Cek konektifitas wireless router ke radius server

5. Lanjutkan dengan mengkonfigurasi wireless router Linksys, Lakukan langkah 1 s/d 5 seperti pada **percobaan I**

7. Pilih **Security Mode** untuk **WPA Enterprise** atau **WPA2 Enterprise.** Kemudian masukkan **IP address** server radius, **radius port** dan **shared key.**



Setting wireless router dengan menggunakan WPA Enterprise

8. Klik tombol “Save Setting” dan ujicobakan pada perangkat wireless client.

E. TUGAS

Kumpulkan hasil percobaan di atas , tambahkan dalam TUGAS tugas berikut ini:

- Buatlah sebuah sistem keamanan wireless dengan mengimplementasikan sistem captive portal dengan menggunakan ***chillispot***