GNOTHI SEAUTON

Pembangunan gedung pencakar langit pasti dimulai dengan peletakan batu pertama. Sebuah perjalanan beribu-ribu mil pasti dimulai dengan langkah pertama. Begitu juga dengan perjalanan dalam hidup ini untuk meraih tujuan yang diidam-idamkan, juga dimulai dengan langkah pertama. Dan langkah pertama untuk meraih keberhasilan tersebut adalah mengenali diri sendiri. Begitu pula dalam melakukan aksi hacking, dengan mengenali diri Anda tentunya Anda siap untuk berperang (melakukan wireless hacking). Dalam buku saya yang berjudul "Buku Sakti Hacker" Anda bisa melihat ada banyak hal yang bisa dilakukan untuk mengenali diri sendiri. Dalam bab ini, kita hanya fokus pada aktivitas wireless hacking saja.

Judul bab ini 'Gnothi Seauton' diambil dari pepatah Yunani kuno yang bermakna 'kenali dirimu sendiri'. Dalam melakukan aksi wireless hacking dalam buku ini, ada baiknya Anda mengenali apa yang ada dalam perangkat komputer Anda sebagai salah satu senjata yang akan Anda gunakan untuk melakukan aksi wireless hacking nantinya. Tentu saja dengan perangkat yang memadai, baik berupa hardware maupun software akan sangat menunjang sekali proses wireless hacking yang akan Anda lakukan.

Gambar 2.1 Gnothi Seauton

Setiap komputer pada jaringan wireless dilengkapi dengan sebuah radio tranceiver, atau biasanya disebut kartu adapter atau wireless adapter, yang akan mengirim dan menerima sinyal radio dari dan ke komputer lain dalam sebuah jaringan. Oleh karena itu, sebelum melakukan kegiatan wireless hacking dalam buku ini, pastikan komputer atau laptop Anda telah memiliki wireless adapter untuk melakukan koneksi ke jaringan wireless. Saya sendiri menggunakan laptop. Supaya mudah dipahami oleh umum, saya menyebut perangkat yang Anda gunakan komputer saja, walaupun Anda menggunakan laptop. Dan sebaiknya Anda mencoba melakukan koneksi pada sebuah jaringan wireless untuk mengetahui bahwa wireless adapter yang Anda miliki bekerja dengan baik. Kalau Anda sudah sering akses internet melalui hotspot, saya rasa Anda tidak perlu melakukan pengujian lagi.

Dalam melakukan aksi wireless hacking, kebutuhan akan wireless adapter tentu saja menjadi syarat wajib yang harus dipenuhi. Mau tidak mau untuk mempraktikkan apa yang disampaikan dalam buku ini, Anda harus memiliki wireless adapter atau disebut juga wireless card pada komputer/laptop. Karena perangkat inilah sebagai perangkat utama dalam melakukan aksi wireless hacking, yang Anda butuhkan untuk menemukan dan berkomunikasi dengan sinyal yang ada pada jaringan wireless.

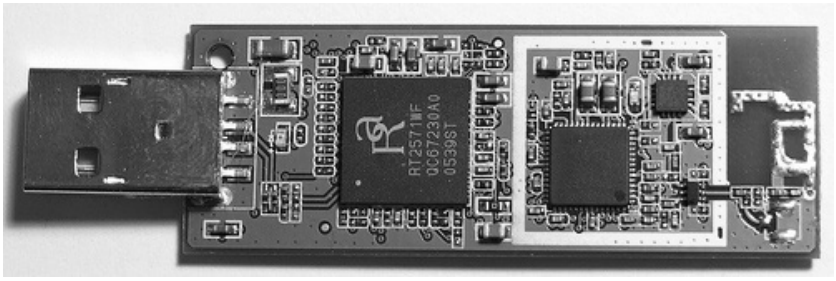
Beberapa wireless adapter dapat kita atur mode-nya. Mode-mode tersebut adalah:

- **Master Mode**. Apabila perangkat wireless kita buat sebagai master, maka perangkat tersebut akan menjadi sebuah access point yang bisa berkomunikasi dengan banyak klien. Dengan menjadi Master Mode maka perangkat memiliki nama pengenal (SSID).
- **Managed Mode**. Mode ini disebut juga dengan Client Mode. Perangkat dengan mode ini hanya bisa berkomunikasi dengan perangkat yang menggunakan mode Master. Channel pada mode ini akan mengikuti channel Master.
- **Ad Hoc Mode**. Tidak ada yang bertindak sebagai access point dalam mode ini. Antar-perangkat dalam mode ini dapat saling berkomunikasi secara langsung. Channel yang digunakan untuk berkomunikasi antarperangkat harus sama.
- **Monitor Mode**. Perangkat dalam mode ini hanya bisa memonitor (melihat atau mendengar) lalu lintas data dalam jaringan.

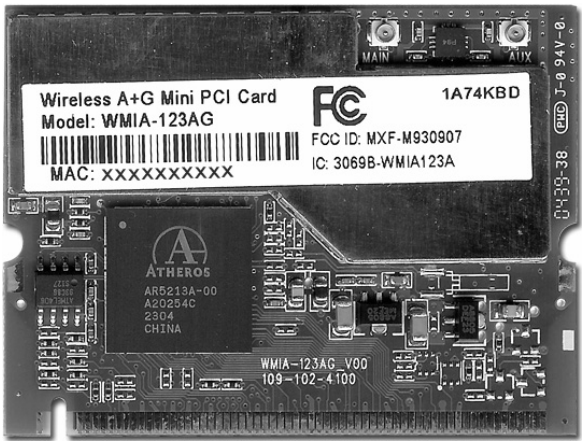
Untuk melakukan aksi hacking, kebutuhan akan wireless adapter tertentu memang diperlukan. Walaupun beberapa bagian dalam buku ini, Anda tetap bisa mempraktikkan isi buku ini tanpa harus menggunakan wireless adapter tertentu. Namun, dengan wireless adapter tertentu tersebut, Anda bisa melakukan aksi wireless hacking lebih optimal. Perangkat utama yang sebenarnya adalah chipset yang terdapat pada sebuah wireless adapter. Terutama sekali chipset wireless adapter yang memiliki kemampuan untuk melakukan monitor dan *packet injection*. Sebab wireless adapter yang mendukung mode monitor dan *packet injection* bisa melakukan lebih banyak aksi hacking nantinya.

Mode monitor merupakan kemampuan menangkap (meng-*capture*) paket data yang bertebaran di udara. Sedangkan mode *packet injection* adalah kemampuan untuk menginjeksi paket-paket dalam sebuah jaringan wireless sehingga Anda bisa mengirimkan paket-paket data tertentu pada access point maupun klien.

Perhatikan gambar di bawah ini, Anda bisa melihat chipset yang digunakan pada wireless adapter.



Gambar 2.2 Chipset wireless adapter
(Sumber: http://farm3.static.flickr.com/2250/2274973919_1da35281dd.jpg)

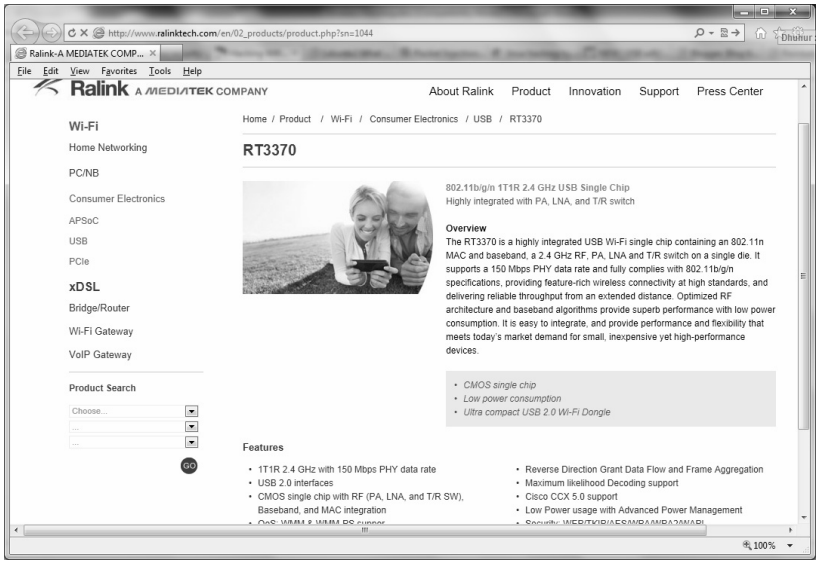


Gambar 2.3 Chipset Atheros
(Sumber: http://werewind.com/pictures/SparkLAN-WMIA-123AG-wirless-802.11abg-Mini-PCI-wifi%20card-Atheros-chipset-AR5004X-AR5213-AR5112-f-m.jpg)

Beberapa chipset wireless adapter yang mendukung kedua hal tersebut adalah:

- Atheros
- Ralink RT73
- Ralink RT2500
- Ralink RT2570
- RALINK 2870/3070
- REALTEK RT 8187

Untuk chipset lainnya, Anda bisa mencari informasinya di website dari wireless adapter yang Anda gunakan.

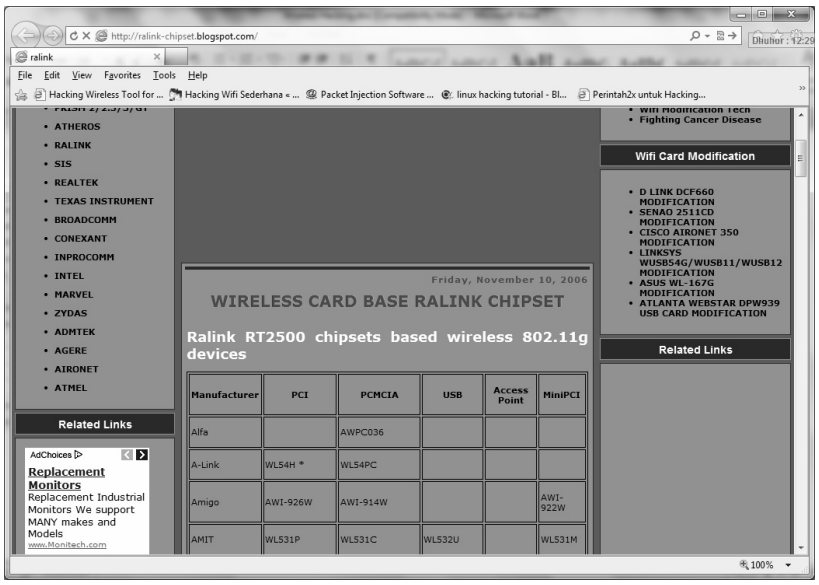


Gambar 2.4 Ralinktech.com

Hal yang agak susah adalah menemukan wireless adapter yang memiliki chipset dengan kemampuan yang bisa digunakan untuk injeksi paket. Dalam hal ini chipset yang paling terkenal, yaitu "Atheros". Tapi tidak semua chipset atheros mendukung injeksi paket, soalnya kita harus mengganti driver bawaannya dengan driver yang support injeksi paket, supaya tidak hanya bisa monitoring saja. Wildpackets dan Tamos adalah perusahaan yang membuat driver untuk wireless adapter supaya bisa melakukan injeksi paket, yaitu AiroPeek dan CommView. Kalau Anda menggunakan produk gratisan alias yang free, saya lebih memilih menggunakan CommView karena versi gratisnya tetap bisa digunakan tanpa banyak batasan, seperti versi gratis dari produk Wildpackets.

Salah satu situs yang bisa dijadikan untuk memperoleh informasi mengenai chipset untuk wireless adapter adalah http://ralink-chipset.blogspot.com/.

Pada bagian sebelah kiri situs tersebut, Anda bisa melihat untuk jenis chipset lainnya, seperti Atheros, SIS, Realtek, dan yang lainnya.



Gambar 2.5 Ralink-chipset.blogspot.com

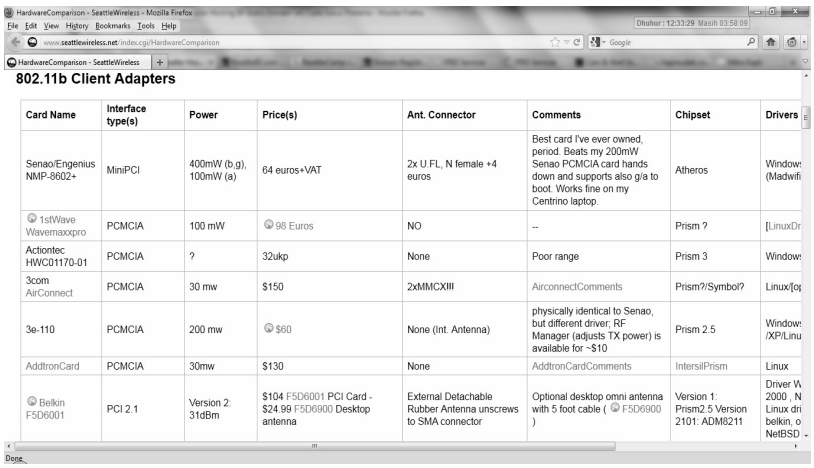
Selain itu, Anda juga bisa mengunjungi beberapa situs di bawah ini untuk melihat beberapa vendor yang menggunakan chipset di atas:

- http://ralink.rapla.net/
- http://atheros.rapla.net/
- http://broadcom.rapla.net/

Selain beberapa situs di atas, Anda juga bisa membuka situs http://www.seattlewireless.net/index.cgi/HardwareComparison.

Dalam situs tersebut ditampilkan informasi mengenai wireless adapter beserta perbandingannya, termasuk juga chipset yang digunakan.

Menurut pengalaman pribadi saya, apabila Anda harus memilih satu chipset wireless adapter dari beberapa chipset yang ada maka saya akan memilih Atheros. Sebab, Atheros bisa berjalan baik di lingkungan Windows maupun Linux. Walaupun demikian, mungkin Anda memiliki pertimbangan lain sewaktu membeli wireless adapter, misalnya harga, driver, manual, kompatibilitas dengan sistem yang Anda gunakan dan sebagainya.

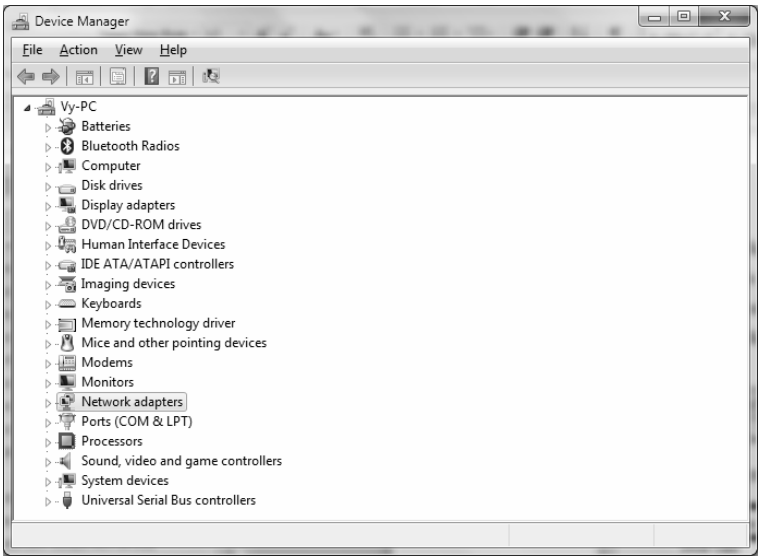


802.11b Client Adapters

Card Name	Interface type(s)	Power	Price(s)	Ant. Connector	Comments	Chipset	Drivers
Senao/Engenius NMP-8602+	MiniPCI	400mW (b,g), 100mW (a)	64 euros+VAT	2x U.FL, N female +4 euros	Best card I've ever owned, period. Beats my 200mW Senao PCMCIA card hands down and supports also g/a to boot. Works fine on my Centrino laptop.	Atheros	Windows (Madwifi
1stWave Wavemaxxpro	PCMCIA	100 mW	98 Euros	NO	--	Prism ?	[LinuxDr
Actiontec HWC01170-01	PCMCIA	?	32ukp	None	Poor range	Prism 3	Windows
3com AirConnect	PCMCIA	30 mw	$150	2xMMCXIII	AirconnectComments	Prism?/Symbol?	Linux/[o
3e-110	PCMCIA	200 mw	$60	None (Int. Antenna)	physically identical to Senao, but different driver; RF Manager (adjusts TX power) is available for ~$10	Prism 2.5	Windows /XP/Linu
AddtronCard	PCMCIA	30mw	$130	None	AddtronCardComments	IntersilPrism	Linux
Belkin F5D6001	PCI 2.1	Version 2: 31dBm	$104 F5D6001 PCI Card - $24.99 F5D6900 Desktop antenna	External Detachable Rubber Antenna unscrews to SMA connector	Optional desktop omni antenna with 5 foot cable (F5D6900)	Version 1: Prism2.5 Version 2101: ADM8211	Driver W 2000 , N Linux dri belkin, o NetBSD

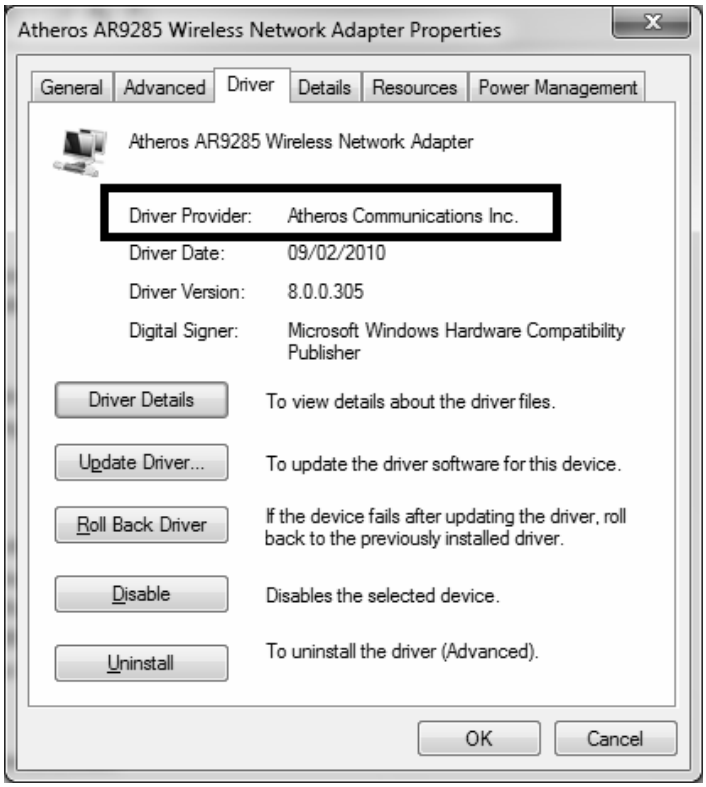
Gambar 2.6
http://www.seattlewireless.net/index.cgi/HardwareComparison

Sekarang kita akan melihat jenis chipset yang digunakan pada wireless adapter Anda. Langkah yang perlu Anda lakukan adalah masuk ke *Device Manager* pada sistem operasi Windows yang Anda gunakan. Lalu perhatikan pada bagian **Network adapters**.



Gambar 2.7 Device Manager

Untuk mengetahui chipset yang digunakan oleh wireless adapter Anda, dalam halaman *Device Manager*, klik dua kali nama wireless adapter yang Anda gunakan. Dari kotak dialog *Properties* yang muncul, klik tab **Driver**. Perhatikan pada bagian *Driver Provider*, itulah nama chipset yang digunakan oleh wireless adapter Anda.



Gambar 2.8 Driver Wireless Adapter

Untuk mengakhiri bab ini, perlu saya sampaikan: "Maaf, saya tidak menerima pertanyaan dari pembaca yang menanyakan, apakah wireless adapter tertentu bagus untuk wireless hacking atau tidak. Ada ribuan merek wireless adapter, jadi tidak mungkin saya harus memeriksa semuanya. Silakan Anda cari di Google, website perusahaan pembuat wireless adapter maupun website lainnya, dan buku manual. Saya juga tidak menerima permintaan untuk melakukan aksi hacking apa pun."