Goodboy, Org.

Unclassified

基于 BT/Kali 的渗透专用无线网卡列表及测试报告

- Show U some Compatible USB Wireless Adapters for BT, Kali, etc.

Summarized by Ray Lee
Blog: http://www.cnblogs.com/webapplee
Date: 2014-11-18
Ver.: 2.1.1

History	
Ray Lee	2014-11-18 V1.0 base article
Ray Lee	2014-11-18 V1.1.2 Release
Ray Lee	2014-11-18 V1.2 Review and modify
Ray Lee	2014-11-18 V2.1 Draft

1. 三种 BT/Kali 专用无线芯片及产品介绍

Intro.: The article is based on BT5/Kali1.0.9 to recommand you on how to choose a best Wireless Network Adapter to general penetration study.

BT(BackTrack) is a very popular free Linux distribution(Based on Debian) that is commonly being used to hack into wireless networks by using Aircrack-ng to crack the WEP/WPA type encryption. The reason why BT is being used instead of Windows is because there are no patched drivers available for Windows that supports metasploit, unless you are willing to fork out $300 or $700 for an AirPcap TX/NX adapter, it's too expensive to afford. So, it is relatively easy to get BT running by installing using UNetbootin/Win32DiskImager and booting up the live version from USB but the most important thing is to make sure that your USB wireless adapter supports monitor mode and packet injection. 选购一种能够支持监控和注入模式的无线适配器才是最重要的，但针对个人开发学习来说，往往其价格不菲。

If you're looking to purchase a fully compatible plug and play USB wireless adapter that works really well with BT/Kali, it can be tricky because some brands with the exact model can have a different chipset for different version numbers. For example, the TL-WN822N USB wireless adapter by TP-LINK comes with 3 versions. The version 1 uses two different chipsets, which is Atheros AR9170 and AR9102 while version 2 has the Atheros AR7010 and AR9287 chipsets, and the latest version 3 uses Realtek RTL8192CU. The chipset on a USB wireless adapter is the most important information but normally is not shown on the product box or even on the device itself. 每个无线适配器根据型号其无线芯片型号会不同，选择时慎重考虑。

To help you in purchasing the correct adapter, here we list the safest USB wireless network adapter that we've tested to have the best plug and play compatibility with BT5, Kali Linux and Aircrack-ng. 下面将会列出测试样本。

You can find a few online resources suggesting some USB wireless adapters that are compatible with BT/Kali, but most of them are either outdated or simply recommend the Alfa AWUS036H which only supports B and G wireless standards but not N. We do not recommended to just blindly purchase any of the newer adapters released and sold by the manufacturers because most likely BT/Kali would not have the updated drivers to support it. 不推荐选购最新的适配器，因生产商未提供基于 BT/Kali 的相应驱动程序，所以会出现无法正常使用的情况。

After testing more than a dozen USB wireless network adapters, we found out that the 3 chipsets listed below are the most stable with BT/Kali. You can click on the hyperlink to see the list of brands that use the chipset. 通过测试发现以下三种芯片型号在 BT/Kali 上的稳定性较佳。

三种无线芯片型号：

- 1. **Atheros AR9271**　 IEEE 802.11B/G/N
- 2. **Ralink RT3070**　 IEEE 802.11B/G/N
- 3. **Realtek RTL8187L**- IEEE 802.11B/G
-

Most of the wireless network adapters listed on the page from the hyperlink above were released a few years back making it difficult to purchase because manufacturers normally releases new products very frequently and phase out the old versions. After screening through the list, here are our recommended USB wireless adapters that have the best compatibility with BT 5, Kali Linux and Aircrack-ng. Alfa prices were taken from Rokland Technologies, an official Alfa distributor in the USA while TP-LINK from ebay.com. 但是以上三种的芯片型号有些陈旧，并且芯片制造商也已推出更佳的芯片和产品，所以本人就根据当下比较通用稳定性列出了以下若干个更加稳定的产品和型号。

1. Atheros AR9271 芯片

相应产品型号：

- Alfa AWUS036NHA – $ 28.97
- TP-LINK TL-WN722N 或者 TL-WN722NC $ 15.99 - ebay 上裸机廉价，但需考虑高额 Shipping 费用；淘宝上目前售价 100 元左右

TP-LINK TL-WN722N USB Wireless Network Adapter

2. Ralink RT3070

相应产品型号：

- Alfa AWUS036NH – (Bigger size) $ 27.99
- Alfa AWUS036NEH – (Smaller size) $ 21.97

Alfa AWUS036NEH USB Wireless Network Adapter

3. Realtek RTL8187L

相应产品型号：

1. AWUS036H – (Bigger size) $ 24.99
2. AWUS036EW – (Smaller size) $ 19.97

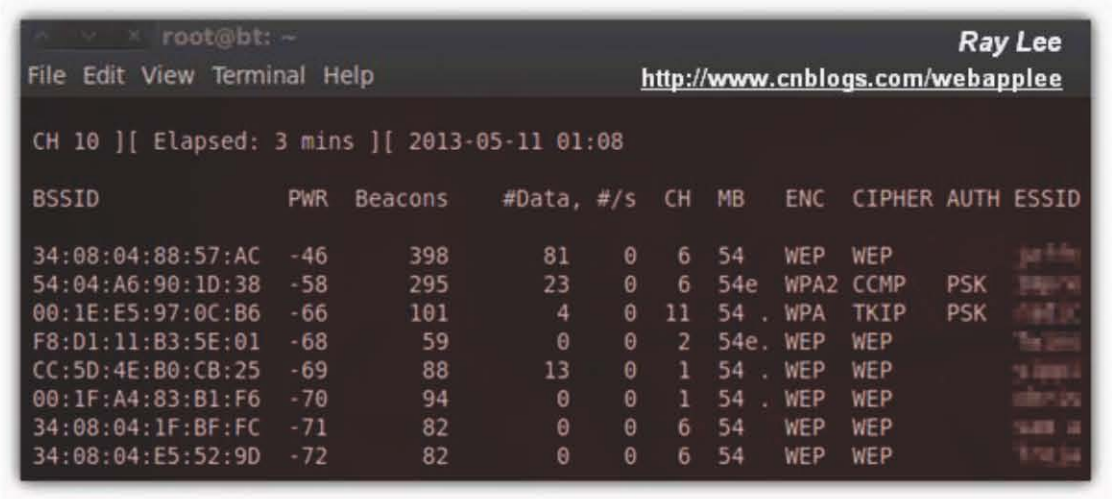
Alfa AWUS036H USB Wireless Network Adapter

2. 相关测试报告：

We’ve put some of the USB wireless adapters mentioned above to the tests to determine the signal performance. 下面将对以上推荐的适配器在 BT/Kali 下进行性能测试。

We’ve managed to test up to 8 wireless network adapters (6 USB + 2 internal) on BT/Kali to determine the signal strength of each device using the command “airodump-ng mon0″ after putting the adapter in monitor mode. Obviously the adapter that detects the most access points with lowest signal level (PWR) deserves to be crowned as the best compatible USB wireless adapter for BT/Kali.

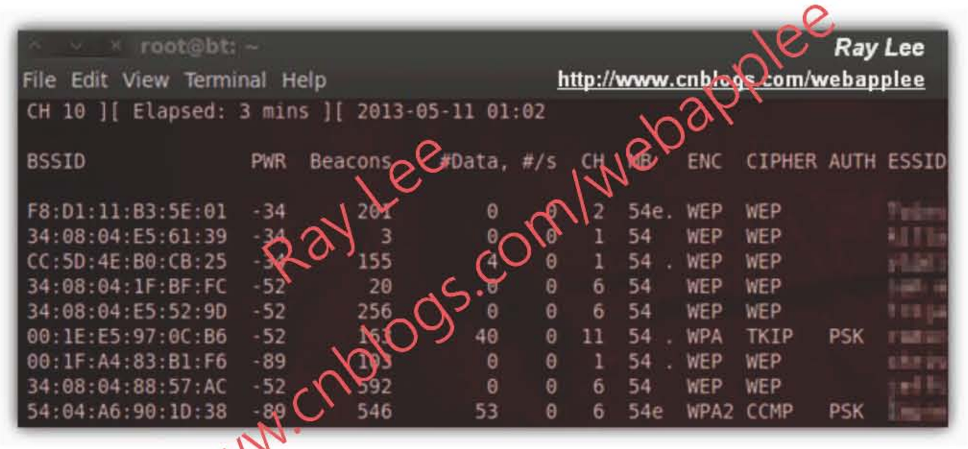
1. **Alfa AWUS036H**



```
CH 10 ][ Elapsed: 3 mins ][ 2013-05-11 01:08

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

34:08:04:88:57:AC  -46      398       81    0   6  54   WEP  WEP         [redacted]
54:04:A6:90:1D:38  -58      295       23    0   6  54e  WPA2 CCMP   PSK  [redacted]
00:1E:E5:97:0C:B6  -66      101        4    0  11  54 . WPA  TKIP   PSK  [redacted]
F8:D1:11:B3:5E:01  -68       59        0    0   2  54e. WEP  WEP         [redacted]
CC:5D:4E:B0:CB:25  -69       88       13    0   1  54 . WEP  WEP         [redacted]
00:1F:A4:83:B1:F6  -70       94        0    0   1  54 . WEP  WEP         [redacted]
34:08:04:1F:BF:FC  -71       82        0    0   6  54   WEP  WEP         [redacted]
34:08:04:E5:52:9D  -72       82        0    0   6  54   WEP  WEP         [redacted]
```

You’ll find that Alfa AWUS036H is the most recommended USB wireless network adapter because it is very stable and works right out of the box for BT. If you don’t mind paying the extra premium price for an adapter with no support for 802.11n wireless standard, then it is quite a good choice. Because Alfa AWUS036H is so popular, there are counterfeit versions being sold online. We recommend you directly contact Alfa Networks if you’re looking for an authorized local distributor. 该产品性能最佳，但缺少 80.211n 协议，针对 n 相关测试无法进行。

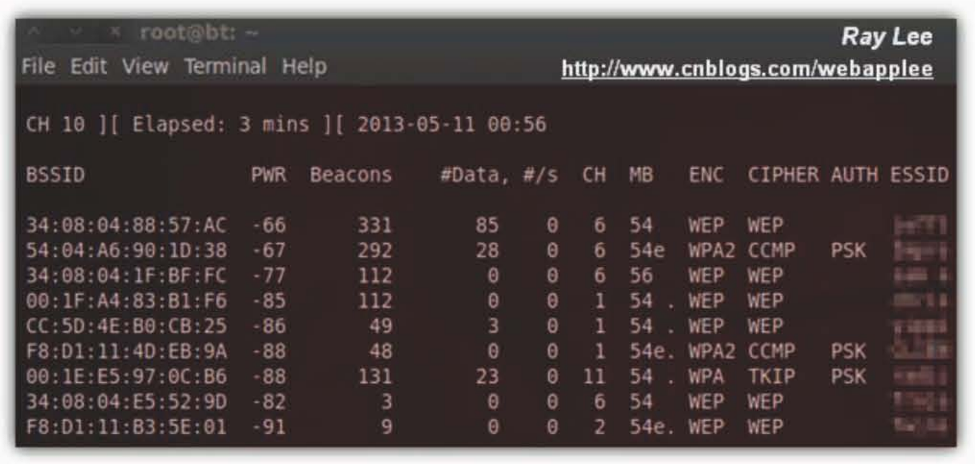
2. **Alfa AWUS036NHR**


root@bt: ~
File Edit View Terminal Help
Ray Lee
http://www.cnblogs.com/webapplee

```
CH 10 ][ Elapsed: 3 mins ][ 2013-05-11 01:02

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F8:D1:11:B3:5E:01  -34      201        0    0   2  54e. WEP  WEP         [redacted]
34:08:04:E5:61:39  -34        3        0    0   1  54   WEP  WEP         [redacted]
CC:5D:4E:B0:CB:25  -34      155        4    0   1  54 . WEP  WEP         [redacted]
34:08:04:1F:BF:FC  -52       20        0    0   6  54   WEP  WEP         [redacted]
34:08:04:E5:52:9D  -52      256        0    0   6  54   WEP  WEP         [redacted]
00:1E:E5:97:0C:B6  -52      163       40    0  11  54 . WPA  TKIP   PSK  [redacted]
00:1F:A4:83:B1:F6  -89      103        0    0   1  54 . WEP  WEP         [redacted]
34:08:04:88:57:AC  -52      592        0    0   6  54   WEP  WEP         [redacted]
54:04:A6:90:1D:38  -89      546       53    0   6  54e  WPA2 CCMP   PSK  [redacted]
```

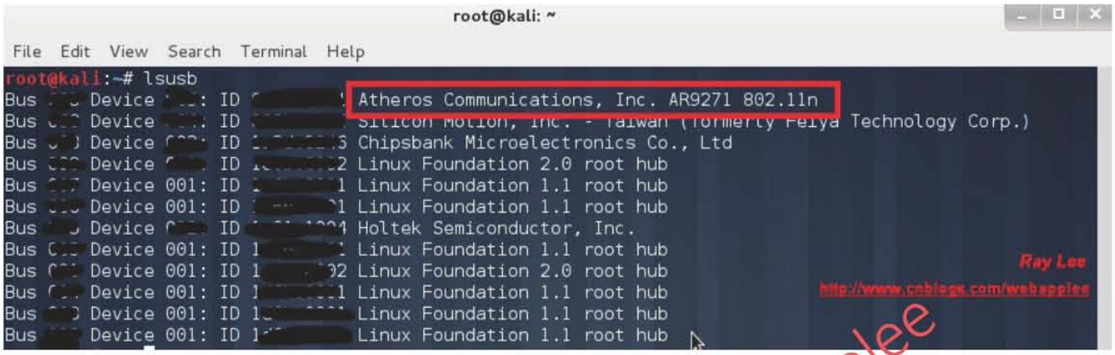
The AWUS036NHR is currently the most powerful wireless adapter by Alfa with very good signal strength. It may seem to be plug and play in BT because you can put it in monitor mode and passes the injection test, but unfortunately it is very unstable because the chipset is not recognized in BT. Alfa 代表作，监控和注入均表现优异，但性能不稳定。

3. **TP-LINK TL-WN722N**


root@bt: ~
File Edit View Terminal Help
Ray Lee
http://www.cnblogs.com/webapplee

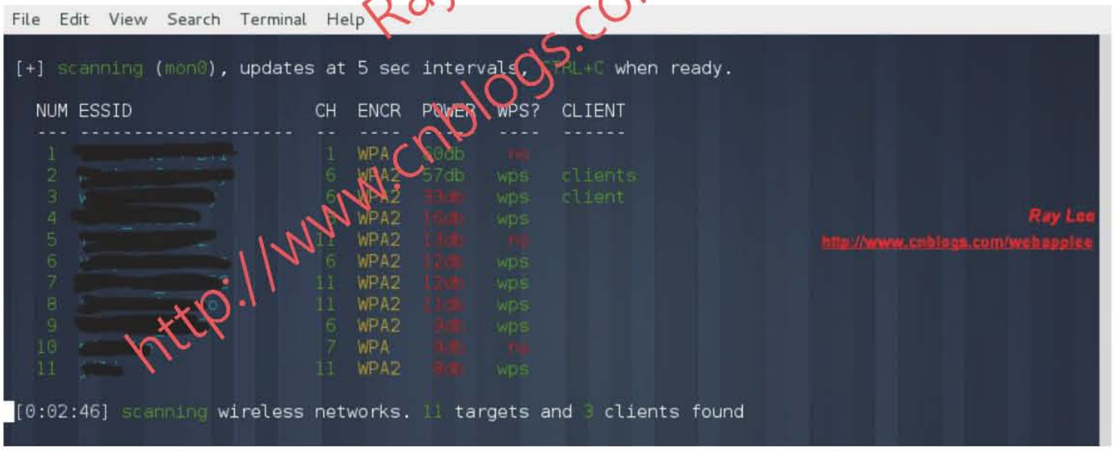
```
CH 10 ][ Elapsed: 3 mins ][ 2013-05-11 00:56

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

34:08:04:88:57:AC  -66      331       85    0   6  54   WEP  WEP         [redacted]
54:04:A6:90:1D:38  -67      292       28    0   6  54e  WPA2 CCMP   PSK  [redacted]
34:08:04:1F:BF:FC  -77      112        0    0   6  56   WEP  WEP         [redacted]
00:1F:A4:83:B1:F6  -85      112        0    0   1  54 . WEP  WEP         [redacted]
CC:5D:4E:B0:CB:25  -86       49        3    0   1  54 . WEP  WEP         [redacted]
F8:D1:11:4D:EB:9A  -88       48        0    0   1  54e. WPA2 CCMP   PSK  [redacted]
00:1E:E5:97:0C:B6  -88      131       23    0  11  54 . WPA  TKIP   PSK  [redacted]
34:08:04:E5:52:9D  -82        3        0    0   6  54   WEP  WEP         [redacted]
F8:D1:11:B3:5E:01  -91        9        0    0   2  54e. WEP  WEP         [redacted]
```

TL-WN722N is a cheaper alternative to the Alfa AWUS036NHA which uses the Atheros AR9271 chipset. It is claimed to be high gain and comes with a 4dBi detachable antenna where you can upgrade to a more powerful antenna to achieve better signal. Although this product was released back in 2009, it is still listed in TP-LINK's official website and can be easily purchased from many sources on the Internet. There is another very similar model which is the TL-WN722NC. It is exactly the same as TL-WN722N except it comes with an additional cradle. 本作者推荐该产品，或许是因为国产，而且相对便宜，性能排第二。


root@kali: ~
File Edit View Search Terminal Help
Ray Lee
http://www.cnblogs.com/webapplee

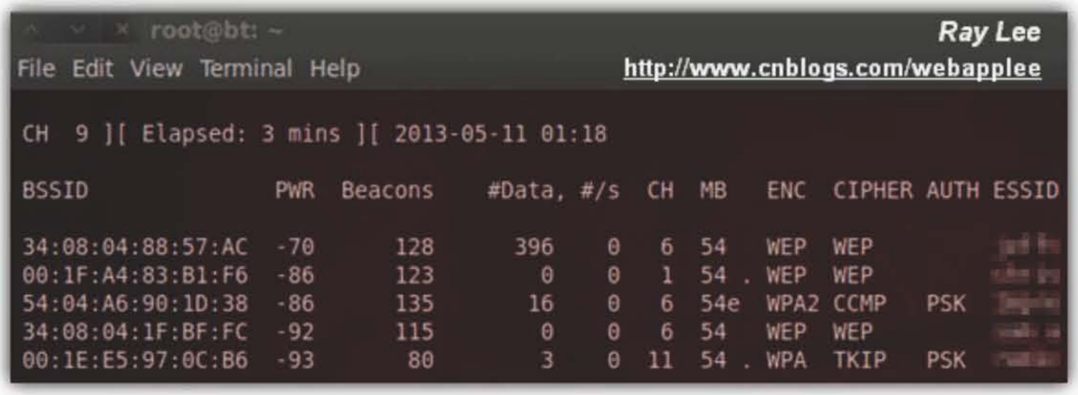
```
root@kali:~# lsusb
Bus [redacted] Device [redacted] ID [redacted] Atheros Communications, Inc. AR9271 802.11n
Bus [redacted] Device [redacted] ID [redacted] Silicon Motion, Inc. - Taiwan (formerly Feiya Technology Corp.)
Bus [redacted] Device [redacted] ID [redacted] Chipsbank Microelectronics Co., Ltd
Bus [redacted] Device [redacted] ID [redacted] Linux Foundation 2.0 root hub
Bus [redacted] Device 001: ID [redacted] Linux Foundation 1.1 root hub
Bus [redacted] Device 001: ID [redacted] Linux Foundation 1.1 root hub
Bus [redacted] Device [redacted] ID [redacted] Holtek Semiconductor, Inc.
Bus [redacted] Device 001: ID [redacted] Linux Foundation 1.1 root hub
Bus [redacted] Device 001: ID [redacted] Linux Foundation 2.0 root hub
Bus [redacted] Device 001: ID [redacted] Linux Foundation 1.1 root hub
Bus [redacted] Device 001: ID [redacted] Linux Foundation 1.1 root hub
Bus [redacted] Device 001: ID [redacted] Linux Foundation 1.1 root hub
```

在 Kali 中的测试结果，各项性能测试性能优异，因其标配外置 4dBi 天线，搜索范围更广，监控和注入测试性能很好，可额外配置更高增益的天线，性能会更佳。


File Edit View Search Terminal Help
Ray Lee
http://www.cnblogs.com/webapplee

```
[+] scanning (mon0), updates at 5 sec intervals, CTRL+C when ready.

  NUM ESSID                 CH  ENCR  POWER  WPS?  CLIENT
  --- --------------------  --  ----  -----  ----  ------
   1  [redacted]             1  WPA   60db    no
   2  [redacted]             6  WPA2  57db   wps   clients
   3  [redacted]             6  WPA2  33db   wps   client
   4  [redacted]    [illegible]  WPA2  16db   wps
   5  [redacted]            11  WPA2  13db    no
   6  [redacted]             6  WPA2  12db   wps
   7  [redacted]            11  WPA2  12db   wps
   8  [redacted]            11  WPA2  11db   wps
   9  [redacted]             6  WPA2   9db   wps
  10  [redacted]             7  WPA    9db    no
  11  [redacted]            11  WPA2   9db   wps

[0:02:46] scanning wireless networks. 11 targets and 3 clients found
```

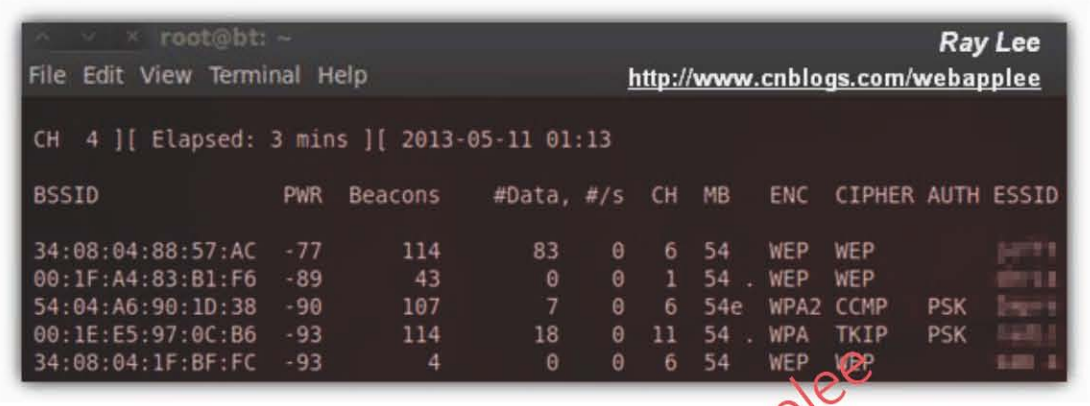
4. ASUS USB-N53


root@bt: ~
File Edit View Terminal Help
Ray Lee
http://www.cnblogs.com/webapplee

```
 CH  9 ][ Elapsed: 3 mins ][ 2013-05-11 01:18

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 34:08:04:88:57:AC  -70      128      396    0   6  54   WEP  WEP         [redacted]
 00:1F:A4:83:B1:F6  -86      123        0    0   1  54 . WEP  WEP         [redacted]
 54:04:A6:90:1D:38  -86      135       16    0   6  54e  WPA2 CCMP   PSK  [redacted]
 34:08:04:1F:BF:FC  -92      115        0    0   6  54   WEP  WEP         [redacted]
 00:1E:E5:97:0C:B6  -93       80        3    0  11  54 . WPA  TKIP   PSK  [redacted]
```

ASUS USB-N53 uses Ralink RT3572 chipset and is fully compatible with BT but is not recommended due to the poor performance. 兼容于 BT，但性能欠佳。

5. **Linksys WUSB600N v2**

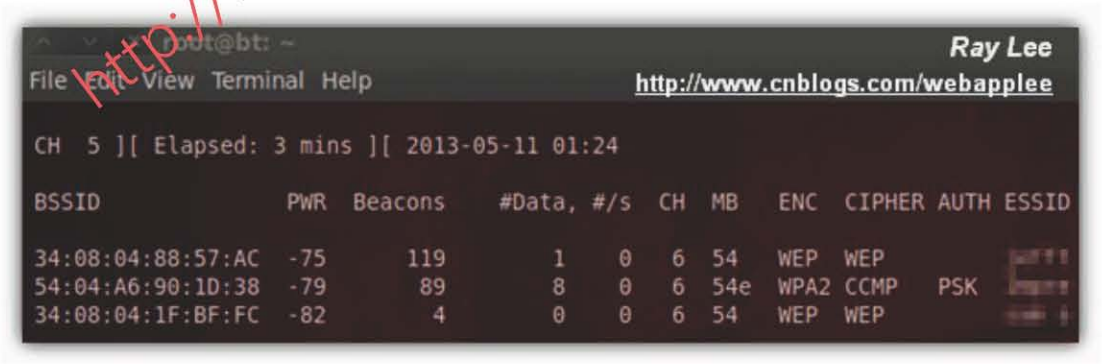


root@bt: ~
File Edit View Terminal Help
Ray Lee
http://www.cnblogs.com/webapplee

```
CH  4 ][ Elapsed: 3 mins ][ 2013-05-11 01:13

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

34:08:04:88:57:AC  -77      114       83    0   6  54   WEP  WEP
00:1F:A4:83:B1:F6  -89       43        0    0   1  54 . WEP  WEP
54:04:A6:90:1D:38  -90      107        7    0   6  54e  WPA2 CCMP   PSK
00:1E:E5:97:0C:B6  -93      114       18    0  11  54 . WPA  TKIP   PSK
34:08:04:1F:BF:FC  -93        4        0    0   6  54   WEP  WEP
```

This USB wireless network adapter uses the same chipset as ASUS USB-N53 which is Ralink RT3572 and has been discontinued. If you check the results at the end of this post, you'd notice that the performance of this adapter with the USB-N53 is very similar. 性能与ASUS USB-N53 类似。

6. **D-Link DWA-110**

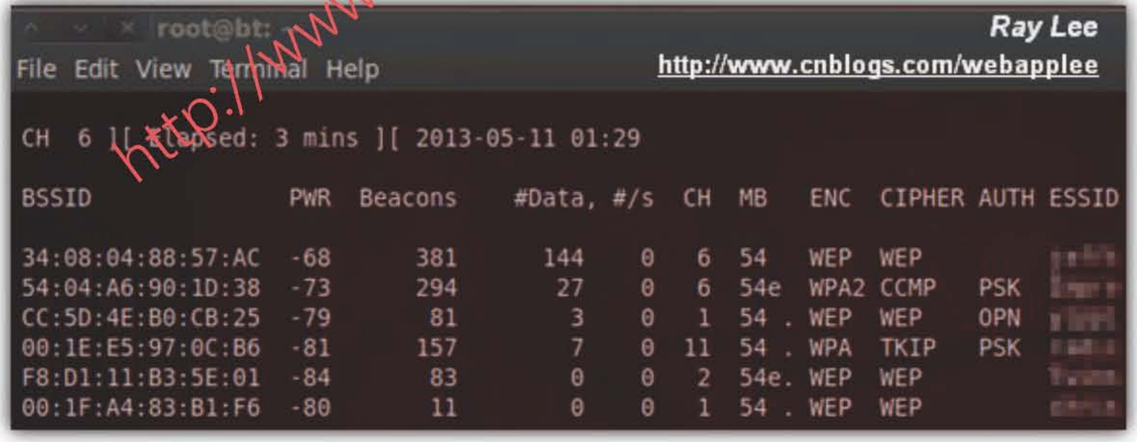


root@bt: ~
File Edit View Terminal Help
Ray Lee
http://www.cnblogs.com/webapplee

```
CH  5 ][ Elapsed: 3 mins ][ 2013-05-11 01:24

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

34:08:04:88:57:AC  -75      119        1    0   6  54   WEP  WEP
54:04:A6:90:1D:38  -79       89        8    0   6  54e  WPA2 CCMP   PSK
34:08:04:1F:BF:FC  -82        4        0    0   6  54   WEP  WEP
```

This adapter is the oldest in the list and it is no surprise that it performed badly on the test. Comparing with the best adapter, DWA-110 merely detected 3 out of 9 access points. 性能很差。

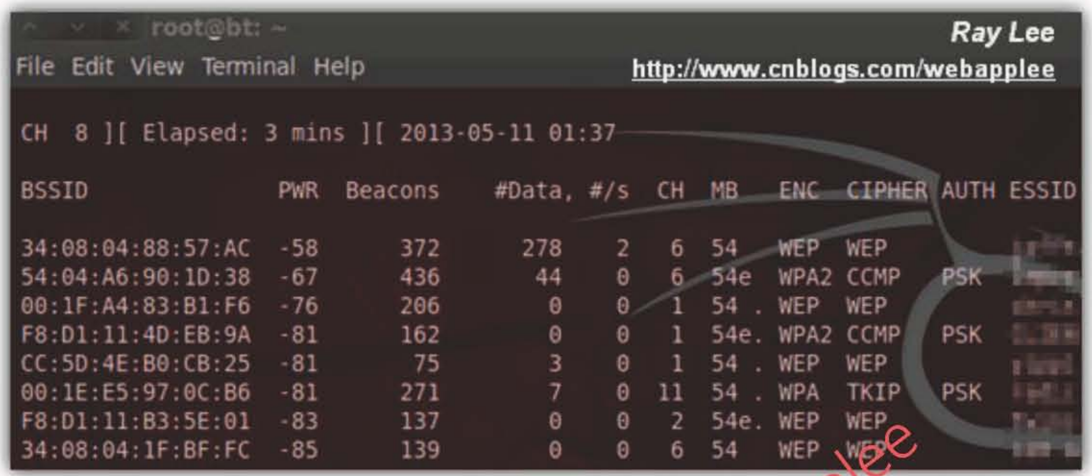
7. **DELL 1510**


root@bt: ~
File Edit View Terminal Help
Ray Lee
http://www.cnblogs.com/webapplee

```
CH  6 ][ Elapsed: 3 mins ][ 2013-05-11 01:29

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

34:08:04:88:57:AC  -68      381      144    0   6  54   WEP  WEP         [redacted]
54:04:A6:90:1D:38  -73      294       27    0   6  54e  WPA2 CCMP   PSK  [redacted]
CC:5D:4E:B0:CB:25  -79       81        3    0   1  54 . WEP  WEP    OPN  [redacted]
00:1E:E5:97:0C:B6  -81      157        7    0  11  54 . WPA  TKIP   PSK  [redacted]
F8:D1:11:B3:5E:01  -84       83        0    0   2  54e. WEP  WEP         [redacted]
00:1F:A4:83:B1:F6  -80       11        0    0   1  54 . WEP  WEP         [redacted]
```

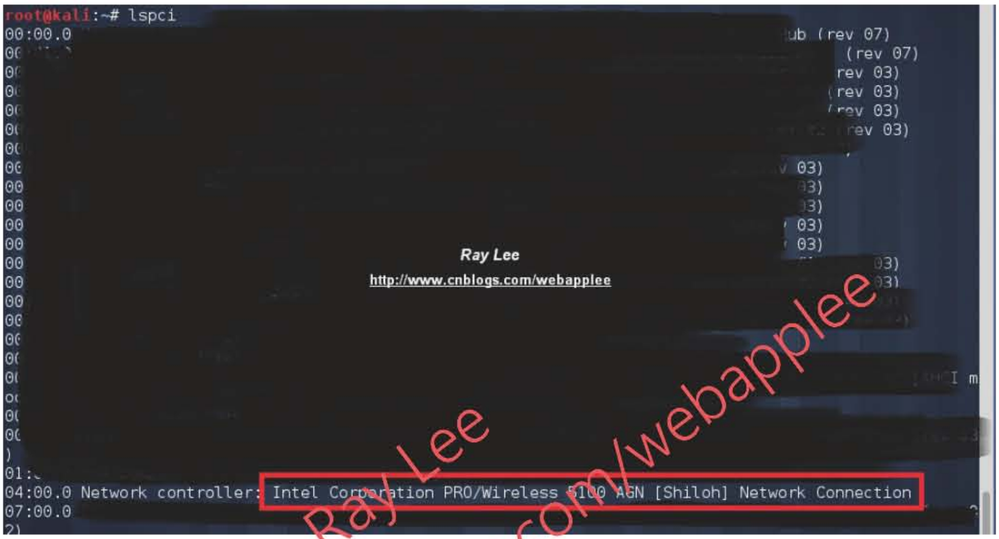
Although it seems to have better performance that some of the external USB wireless adapters, only monitor mode works but not injection due to the Broadcom chipset. 基于博通 BCM94322 特有系列芯片，兼容性稍差，不支持监控模式，性能不错。

8. **Intel 5100**


root@bt: ~
File Edit View Terminal Help
Ray Lee
http://www.cnblogs.com/webapplee

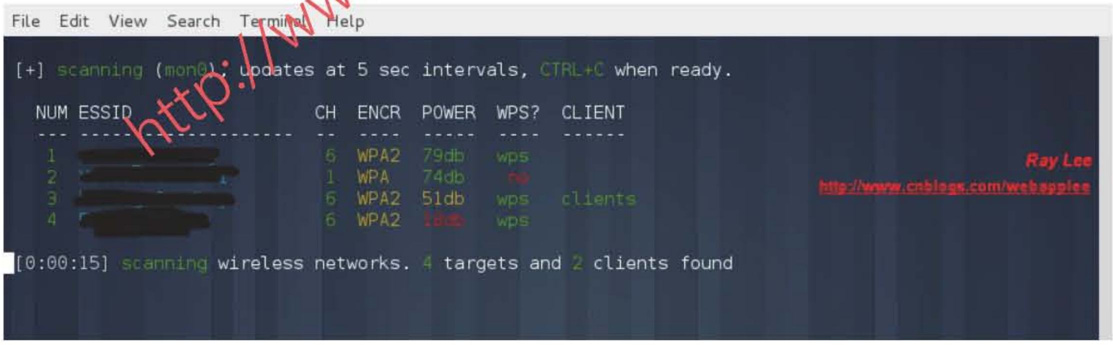
```
CH  8 ][ Elapsed: 3 mins ][ 2013-05-11 01:37

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

34:08:04:88:57:AC  -58      372      278    2   6  54   WEP  WEP         [redacted]
54:04:A6:90:1D:38  -67      436       44    0   6  54e  WPA2 CCMP   PSK  [redacted]
00:1F:A4:83:B1:F6  -76      206        0    0   1  54 . WEP  WEP         [redacted]
F8:D1:11:4D:EB:9A  -81      162        0    0   1  54e. WPA2 CCMP   PSK  [redacted]
CC:5D:4E:B0:CB:25  -81       75        3    0   1  54 . WEP  WEP         [redacted]
00:1E:E5:97:0C:B6  -81      271        7    0  11  54 . WPA  TKIP   PSK  [redacted]
F8:D1:11:B3:5E:01  -83      137        0    0   2  54e. WEP  WEP         [redacted]
34:08:04:1F:BF:FC  -85      139        0    0   6  54   WEP  WEP         [redacted]
```

Interestingly the Intel 5100 did quite well and the performance is comparable to the TL-WN722N. However do note that the TL-WN722N uses a 4dBi antenna in this test which can be upgraded to a better one to achieve better signal strength. Both monitor mode and packet injection works perfectly. 性能与 TL-WN722N 4dBi 标配相似，但 TL-WN722N 可外置更高增益的天线，所以推荐 TL-WN722N。



```
root@kali:~# lspci
00:00.0 [redacted]
04:00.0 Network controller: Intel Corporation PRO/Wireless 5100 AGN [Shiloh] Network Connection
07:00.0 [redacted]
```

在 Kali 中的测试结果不错，各项性能测试无误。



```
[+] scanning (mon0), updates at 5 sec intervals, CTRL+C when ready.

  NUM ESSID                 CH  ENCR  POWER  WPS?  CLIENT
  --- --------------------  --  ----  -----  ----  ------
   1  [redacted]             6  WPA2  79db   wps
   2  [redacted]             1  WPA   74db    no
   3  [redacted]             6  WPA2  51db   wps   clients
   4  [redacted]             6  WPA2  18db   wps

[0:00:15] scanning wireless networks. 4 targets and 2 clients found
```

3. Results and Summary

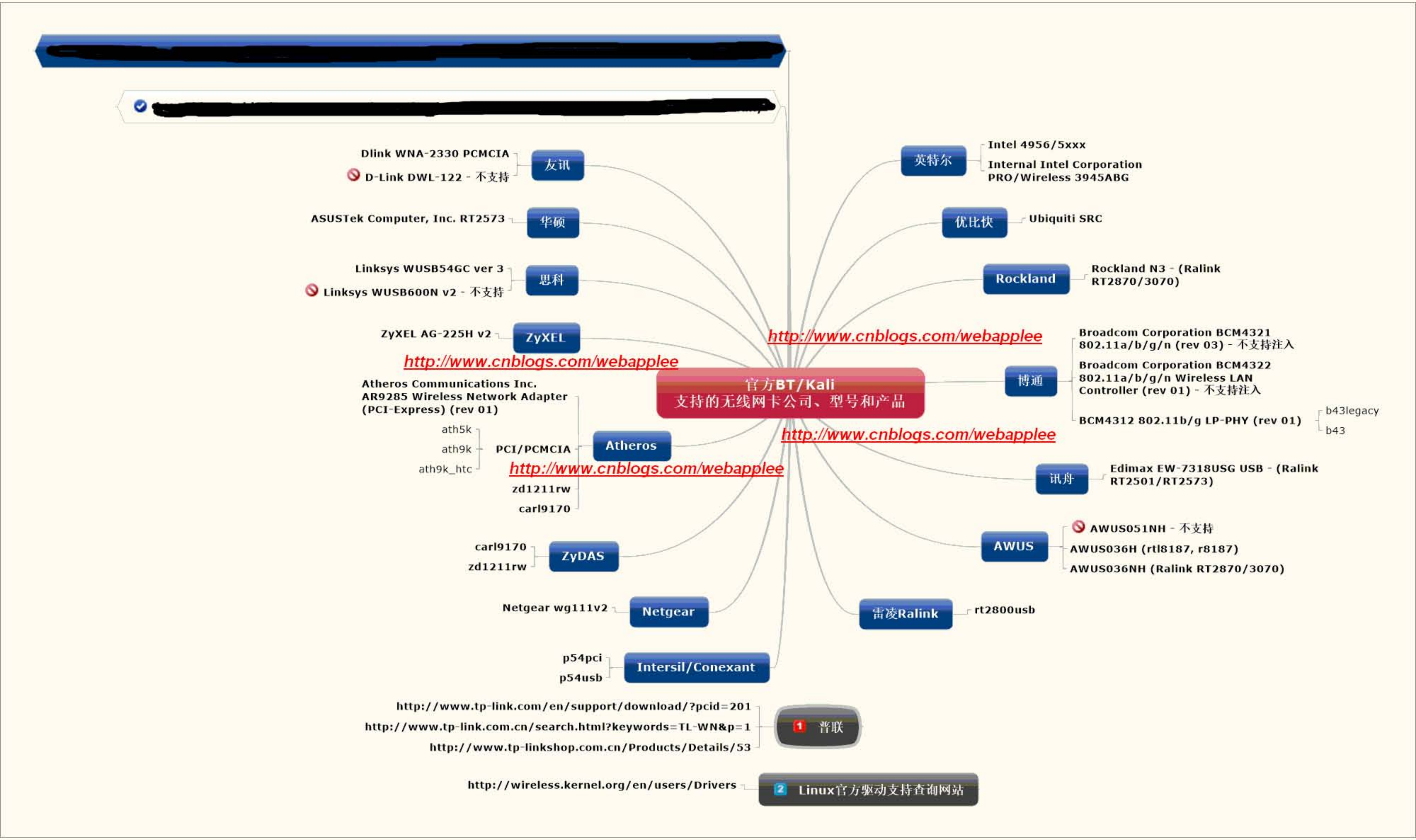
The result table below shows the number of access points the adapters can detect and also the lowest signal level.

无线网卡	搜索 AP	最低信号率(PWR)
Alfa AWUS036NHR	9	-34
Alfa AWUS036H	8	-46
ASUS USB-N53	5	-70
D-Link DWA-110	3	-75
DELL 1510	6	-68
Intel 5100	8/4	-58/18
Linksys WUSB600n v2	5	-77
TP-Link TL-WN722N	9/11	-66/8

BT/Kali 搜索 AP 测试结果表

Summary:

Although AWUS036NHR is the successor of the popular AWUS036H which has better signal strength, unfortunately it is currently not supported on BT. Alfa AWUS036H is still the best choice, followed by TP-LINK TL-WN722N especially if you can get a higher dBi antenna. There is no harm trying out your internal card to see if it works on BT/Kali but take note that internal cards will only work on Live CD/USB but not on virtual machine such as VirtualBox/VMware. Alfa 系列网卡，性能最佳，但国内目前很难买得到，如果需要可以通过 ebay、amazon 等国外知名购物网站购买，要比国内便宜些，但海运比较贵，可以考虑，并看好国内的知名品牌网卡，可以根据**附录**中的网卡芯片支持图中进行选择；电脑内置的无线网卡无法在虚拟机中实现 wifi 测试，故需要额外配置无线网卡，或者通过 U 盘/硬盘的 Live 版本来使用电脑内置的无线网卡。



[redacted]

[redacted]

官方BT/Kali
支持的无线网卡公司、型号和产品

- 友讯
  - Dlink WNA-2330 PCMCIA
  - D-Link DWL-122 - 不支持
- 华硕
  - ASUSTek Computer, Inc. RT2573
- 思科
  - Linksys WUSB54GC ver 3
  - Linksys WUSB600N v2 - 不支持
- ZyXEL
  - ZyXEL AG-225H v2
- Atheros
  - Atheros Communications Inc. AR9285 Wireless Network Adapter (PCI-Express) (rev 01)
  - PCI/PCMCIA
    - ath5k
    - ath9k
    - ath9k_htc
  - zd1211rw
  - carl9170
- ZyDAS
  - carl9170
  - zd1211rw
- Netgear
  - Netgear wg111v2
- Intersil/Conexant
  - p54pci
  - p54usb
- 英特尔
  - Intel 4956/5xxx
  - Internal Intel Corporation PRO/Wireless 3945ABG
- 优比快
  - Ubiquiti SRC
- Rockland
  - Rockland N3 - (Ralink RT2870/3070)
- 博通
  - Broadcom Corporation BCM4321 802.11a/b/g/n (rev 03) - 不支持注入
  - Broadcom Corporation BCM4322 802.11a/b/g/n Wireless LAN Controller (rev 01) - 不支持注入
  - BCM4312 802.11b/g LP-PHY (rev 01)
    - b43legacy
    - b43
- 讯舟
  - Edimax EW-7318USG USB - (Ralink RT2501/RT2573)
- AWUS
  - AWUS051NH - 不支持
  - AWUS036H (rtl8187, r8187)
  - AWUS036NH (Ralink RT2870/3070)
- 雷凌Ralink
  - rt2800usb
- 1 普联
  - http://www.tp-link.com/en/support/download/?pcid=201
  - http://www.tp-link.com.cn/search.html?keywords=TL-WN&p=1
  - http://www.tp-linkshop.com.cn/Products/Details/53
- 2 Linux官方驱动支持查询网站
  - http://wireless.kernel.org/en/users/Drivers

http://www.cnblogs.com/webapplee

http://www.cnblogs.com/webapplee

http://www.cnblogs.com/webapplee

http://www.cnblogs.com/webapplee