I fell on my nose

or

"How to get more from wardriving"

Wireless ARP Poisoning with Cain and Abel

by morning_wood & [ill]will

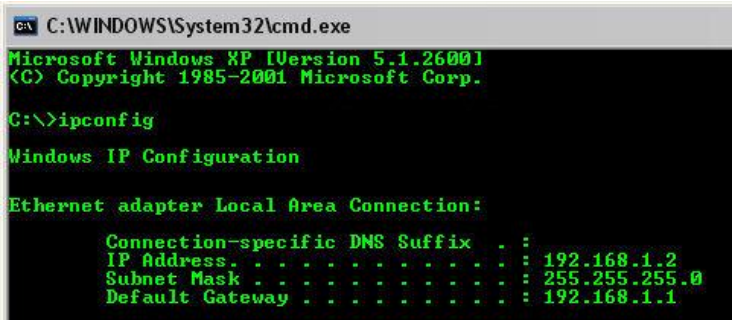
So, you went wardriving/biking/skating/flying whatever, however you do it i dont care. Ok, now your back and you got a GREEN signal and you got a IP (probably private) but you find cant browse the web (because of the private ip). So you figure a you cant do anything with the AP and move on...The techniques are quite simple once you assume a few things when you get connected to a wireless (or LAN) network.

1. You now have (most probably) a private IP address
2. Some internal (LAN) networks assume border routing to NAT to protect against major exploitsand are thus internal clients are often unpatched against things like RPC - WEBDAV - and open shares, etc.
3. You are now connected via the internal networks GATEWAY

tools:
1. Wifi Card
2. Cain and Abel
3. some exploits

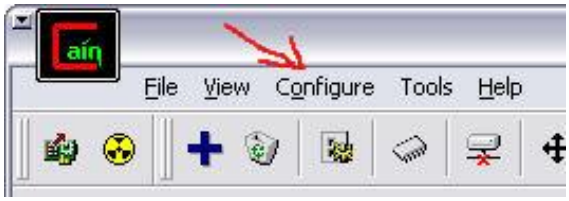
How to make ownage.

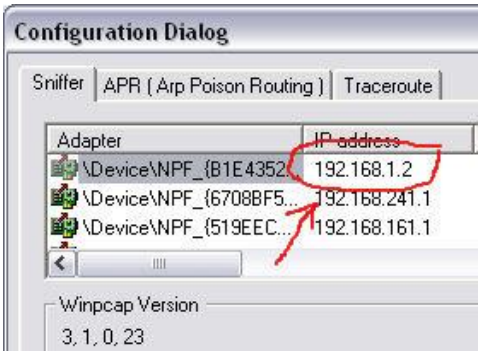
Ok, you got a ip like 192.168.1.2 and running ipconfig you get:



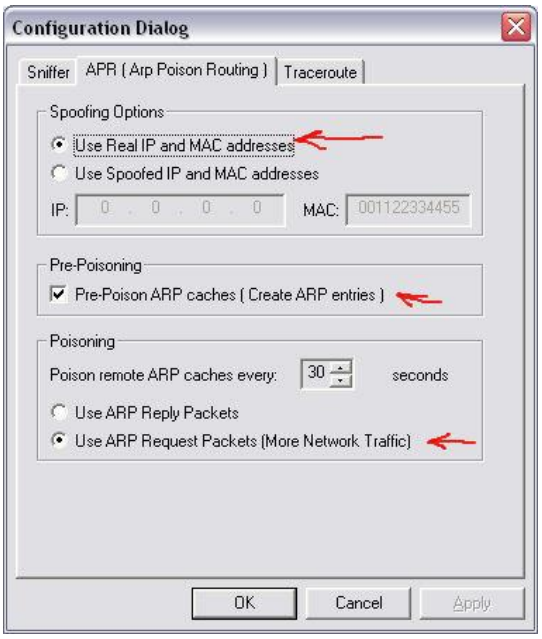
Fire up Cain and Abel.

1. click: configure, sniffer verify that your ip matches that in ipconfig





2. APR, (its OK to use your real mac)
   [x] pre poisoning
   [x] Use ARP Request blabla



note: Cain has no function to change the spoofed MAC from its menu. You may change this in the Windows registry. Or use SMAC

click "OK"

click the ethernet card icon on the left

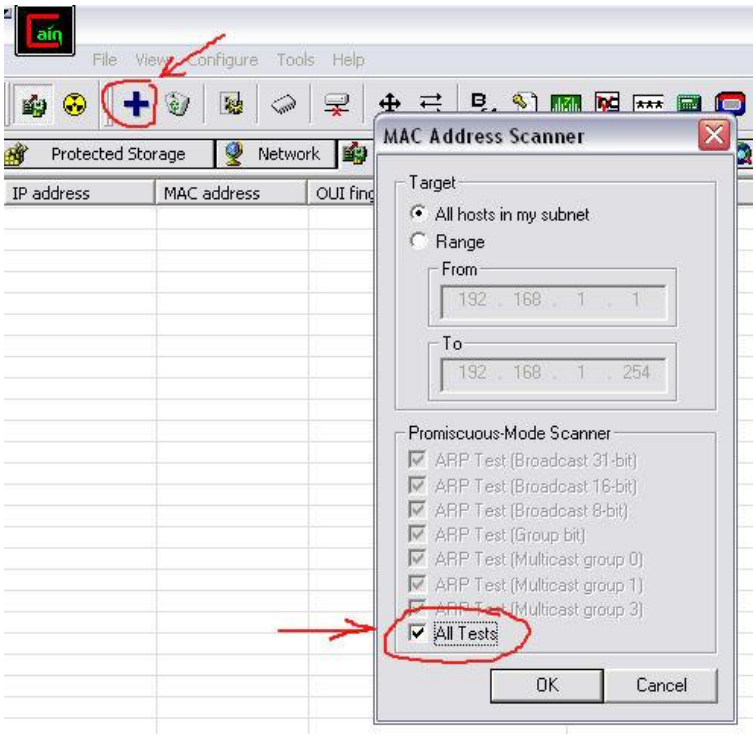
Select menu tab "Sniffer", lower tab "Hosts"

click the BIG BLUE "+"

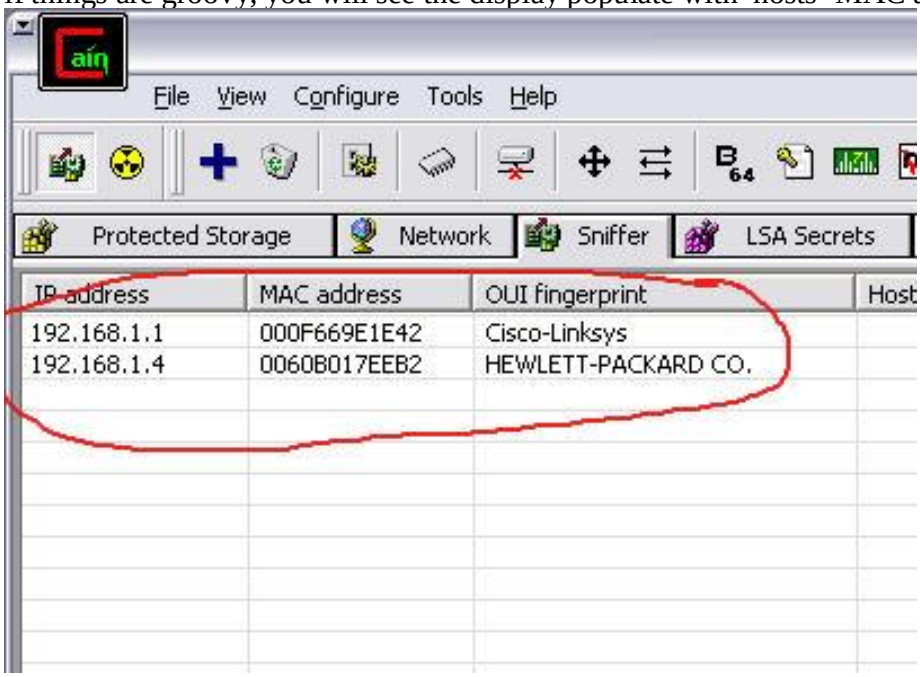
[x] All hosts blabla

[x] All tests

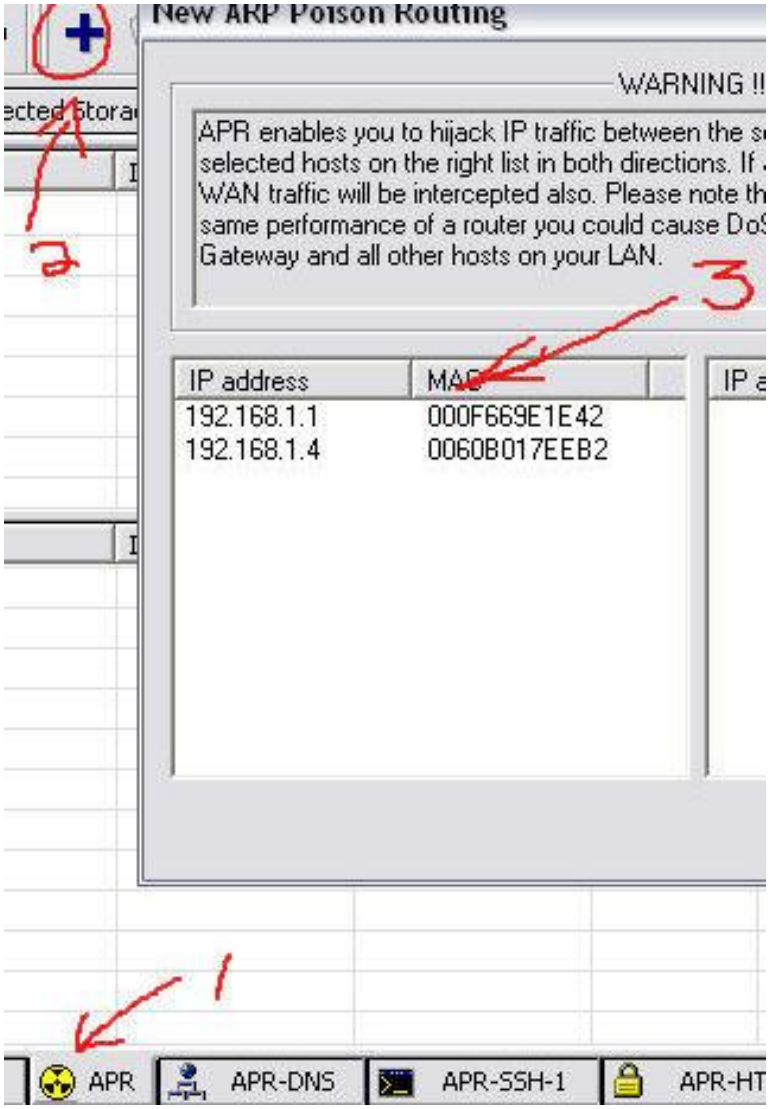
Click "OK"



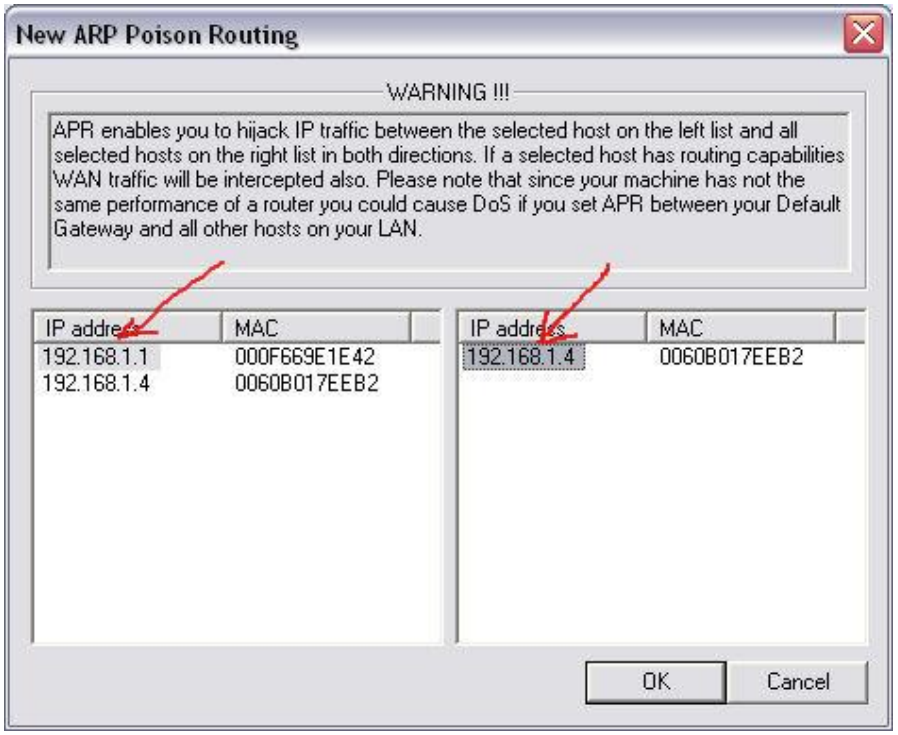
if things are groovy, you will see the display populate with hosts' MAC addresses.



ok, now, lower tab APR, click the BIG "+"

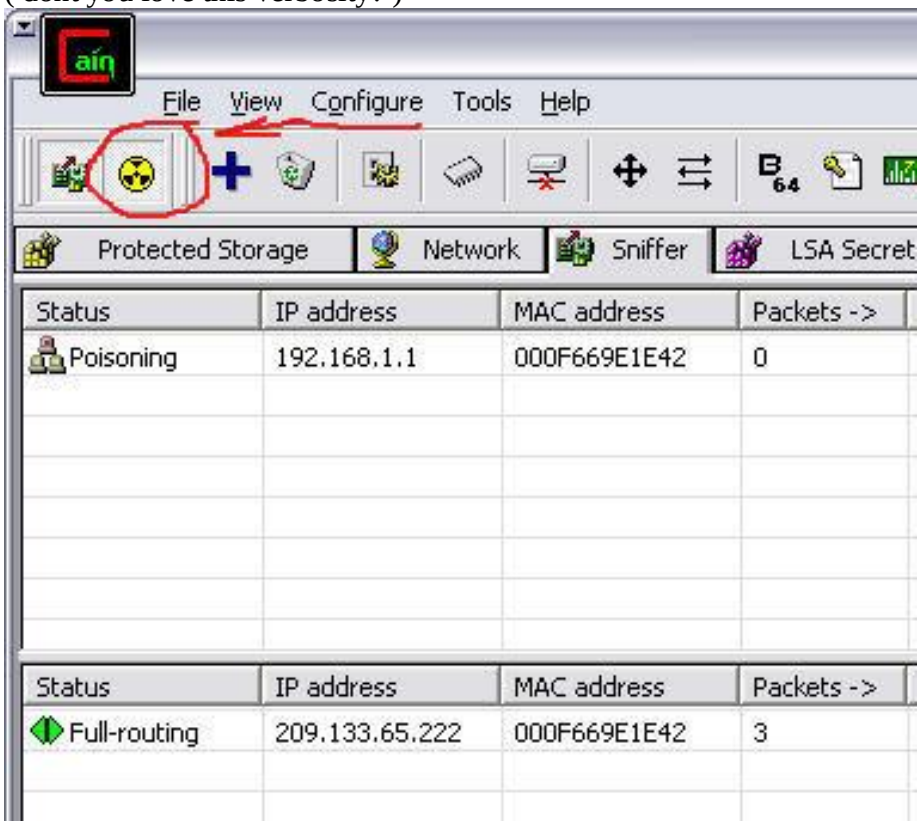


you should be looking at a new dialog box with (hopefully) a row of IP/MAC combinations. find the likely router (hint: i bet its your GATEWAY entry in IPCONFIG) highlight it. all other IP/MAC combo's should be on the right., select them all.



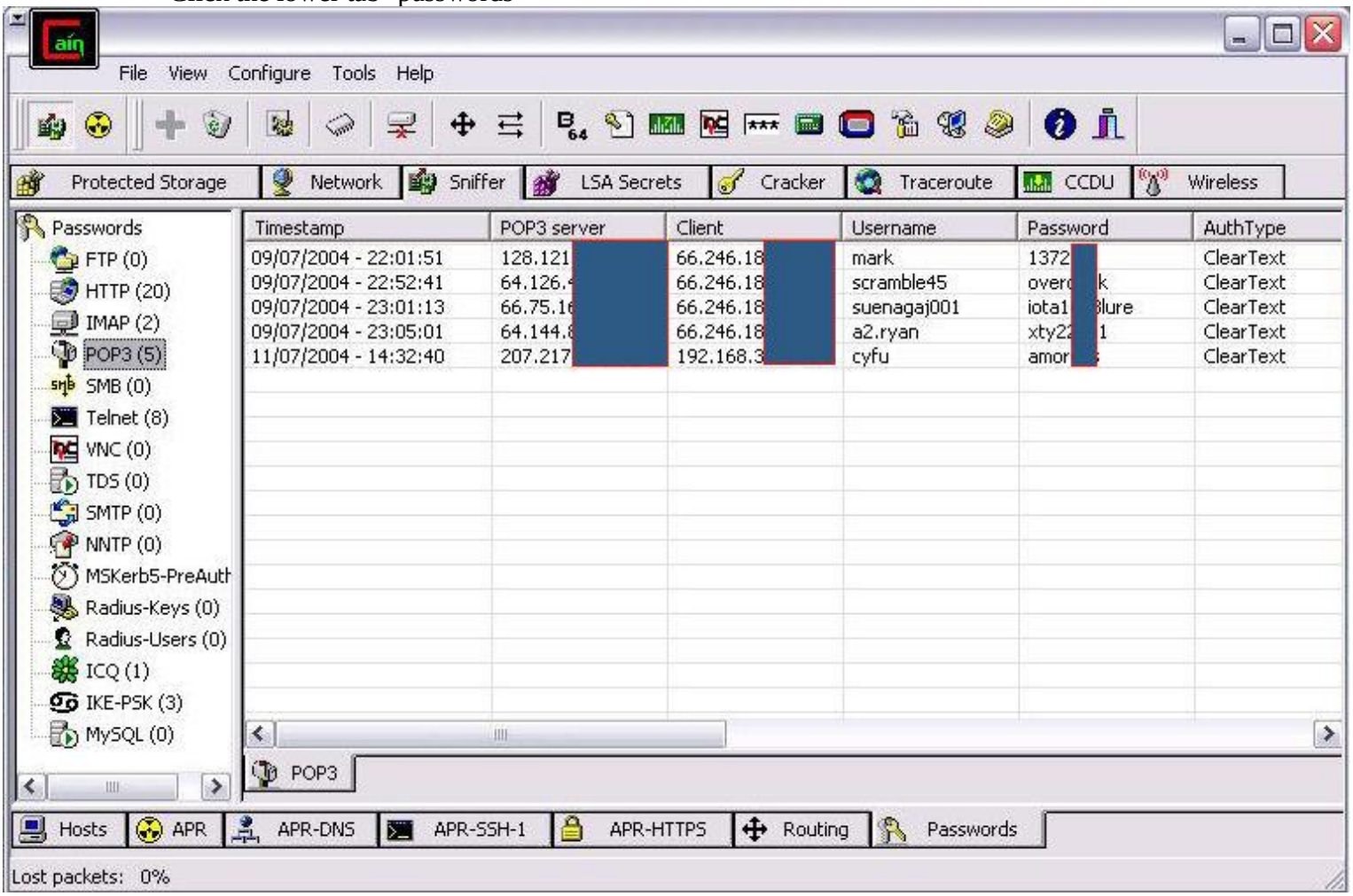
Click "OK"

click the nuke icon next to the ethernet card icon
(dont you love this verbosity?)



You are now ARP poisoning. :D

Click the lower tab "passwords"



from here i leave you to your own skill. (or lack of) the main thing is to be creative, and have permission to evaluate the wireless network in question. ;)

have phun :)

Credits:
morning_wood - http://exploitlabs.com & [ill]will - http://illmob.org
irc.slashnet.org #illmob

greetz:
http://governmentsecurity.org , http://security-wireless.info
http://zone-h.org , http://www.pingywon.com

links:
Cain - http://oxid.it

p.s. thanx to the people attending Hope2k4 for the ‘real-time’ password screenshots