

Switch, Hub, & Monitor

By,

Brian Wilson

CCNA, CCSE, CCAI, MCP, Network+

Slimjim100@gmail.com

www.anti-hacker.info

www.middlegeorgia.org

Introduction: Check list time!

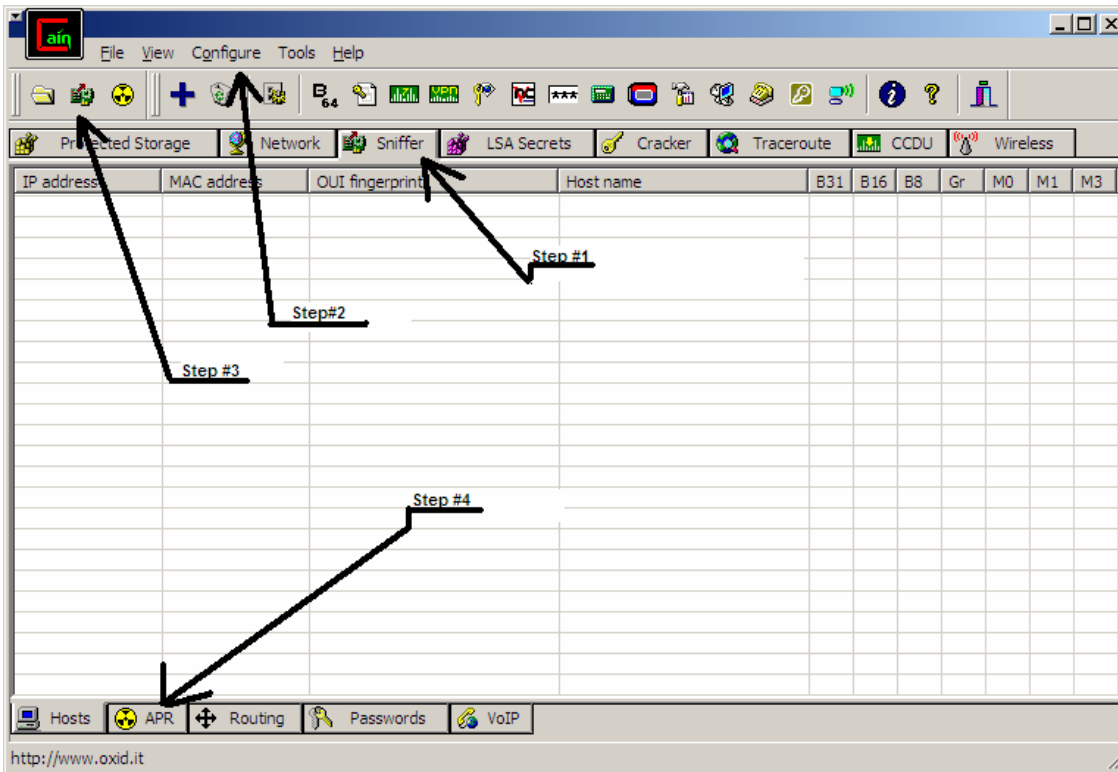
If you are a Network Engineer, IT Consultant, or anyone else that might need to sniff a network to analyze traffic you should know the importance of a monitor or mirror port on a switch. With manageable switches (normally the more costly ones) you have the ability to make a port do monitoring or mirroring (sometimes its even called trunking). When you have monitoring enabled you can see all network traffic on all the ports over the monitoring port as if you were using a hub. This allows you to troubleshoot issues on the network like viruses, IP/MAC conflicts, Spanning tree storms, squawking NIC's, routing/switching loops, and a host of other issues. The problem most of us run into is that the network has a cheap non-manageable switch and you are only able to sniff traffic bound to your NIC & broadcast traffic. The best remedy I have found for this is to Man-In-The-Middle Attach the network to force all the traffic to router/switch through your computer's NIC. Now this is a hacking technique and you should be aware that by launching a Man-In-The-Middle Attach (MITMA) you could be breaking the law. When you launch a MITMA on a network you are Spoofing the Gateway and host on the network to route/switch through your computer so one of the things you should think about (other than do you have the authority to do so) is does your computer have the bandwidth and processor power to handle the traffic you are about to force through it and also is there an IDS (or Switch with security/Anti-Spoofing) in the network that will alarm. After you work out the logistics about the impact of your MITMA you need to test run it to see how the network will react to the ARP Storm you will cause by Spoofing (ARP Poisoning) the LAN. The idea here is to test during off peak hours to see if the network can handle the strain of your computer rewriting the ARP table. Once you have verified that the network can handle this you can move on to setting up the test. The test here consists of the MITMA and then using a protocol sniffer to see what is happening on the network. In the next section I will explain how to carry out this test.

Attach: The moment of truth...

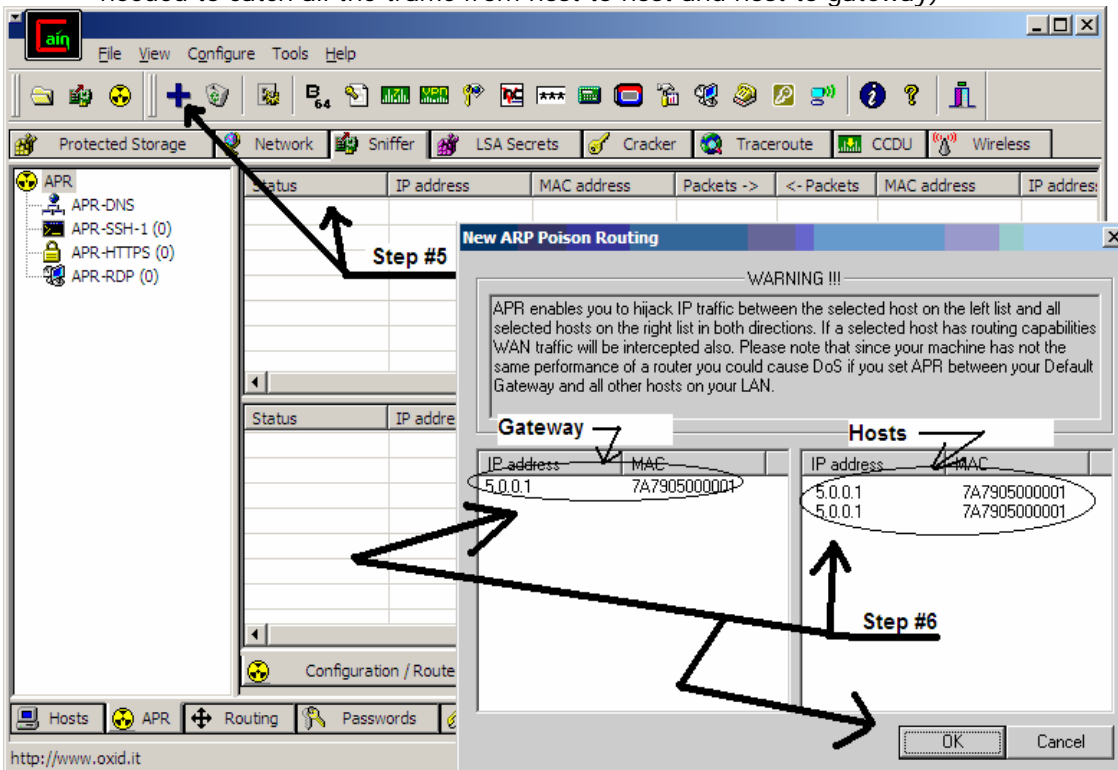
Now that you have covered all the ground work and are sure you are allowed to MITMA the network for testing you need to get the tools for the job. I have a list of tools I recommend for users that enjoy a GUI. I use Cain & Able (www.oxid.it) for the MITMA portion and ethereal (or Wireshark) for the sniffing. You can use a lot of other command line ARP Poisoning tools if you like but I enjoy the GUI tools plus it helps new users understand what they are doing. First thing you need is to setup Cain to ARP Poison on the network. There is a very nice read me file in Cain that will walk you through the setup.

Steps for ARP Poisoning with Cain

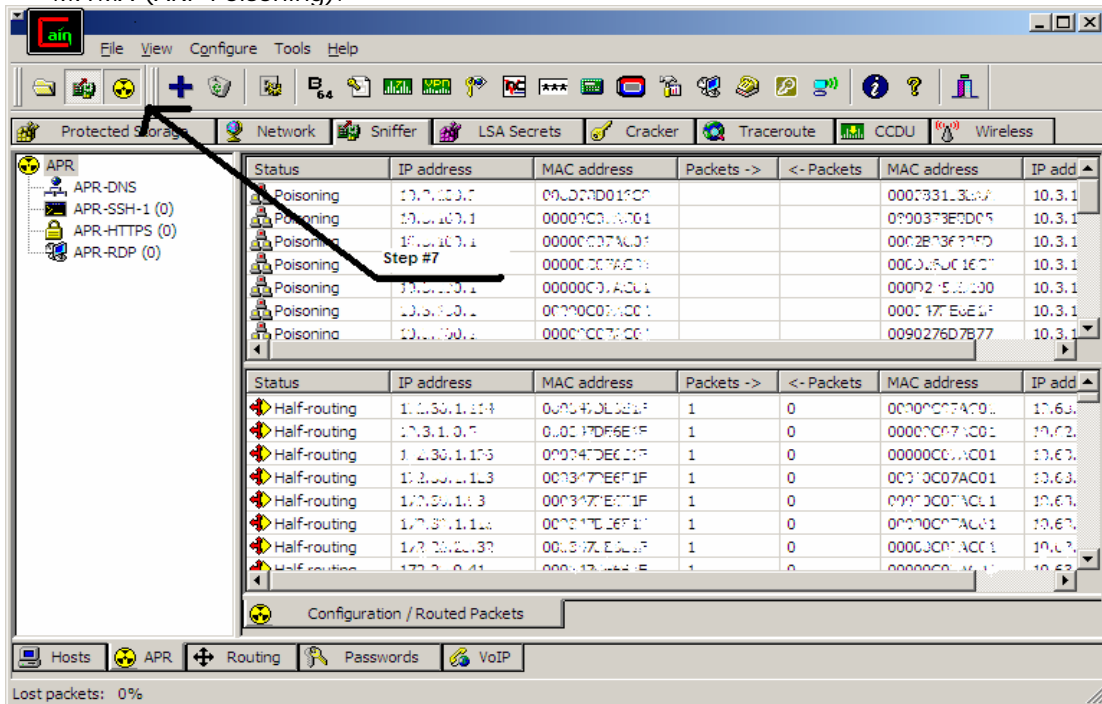
1. Launch Cain and go to the sniffer tab (upper tab)
2. Click on configure and select the NIC you are going to use. (it will show the subnet the NIC is on)
3. Enable the sniffer by pushing the sniffer button. Now right click in the cells and select scan hosts!
4. Go to the bottom tab "ARP"



5. Now you need to Click in the upper cells to activate the "+" sign.
6. now a new window appears and here is where you pick the gateway and hosts. You need to select the one IP from the gateway side and then highlight all the host in the host window and click OK. (you will do this for every IP in the gateway section till you have every combination of gateway to host selection this will take time but it is needed to catch all the traffic from host to host and host to gateway)



- Now that you have all the host selected you need to push the ARP button to start the MITMA (ARP Poisoning).



- At this point you are poisoning the networks ARP tables & your MITMA is active. Keep an eye out for the lost packets status located in the button left corner of Cain. If you see the packet loss go above 5% the result can be slow network performance or even a total switch lock-up so be very careful and if you notice this you should unclick the APR button which will stop the poisoning.

Now on to the sniffing!

At this point you have got the MITMA working and all network traffic is now routed/switched through your computer's NIC. It is time to start the sniffing. You can use any protocol sniffer you like (I use ethereal or Wireshark to sniff) just turn on the sniffer and select the NIC which you are performing the MITMA on. You will see a lot of traffic on this interface and be careful not to overwork your computer's CPU. It is recommended not to sniff too long (if network traffic is heavy your computer might drop packets so be alert). Once you have finished your sniffing use the Protocol sniffers filter to find what packets interest you.

Conclusion: Now you have the data you always wanted...

So with all the steps above followed you are now able to use a few free tools and a laptop to sniff and analyze network traffic. If you were to buy a hardware sniffer to do this it would cost a lot of money and might not be able to do as much as what I have shown you above. Enjoy the tools have fun and always be careful of sniffing on the network. There are real risks you face when you perform a MITMA on a network and keep in mind the legal and service impacts of doing this. Just as a little side note if your LAN is running VoIP you may want to be extra cautious because if you slow or drop traffic on a VoIP network you will be dropping calls. Cain & Able is a very powerful tool and has hundreds of uses beyond a password sniffer. Just remember that there are a lot of free tools on the internet and combining them can give you a lot of new and useful tools you might not have thought about prior. If you have any questions feel free to e-mail me.