

Own your LAN with Arp Poison Routing

By: Rorik Koster
April 17, 2006

Security is a popular buzzword heard every day throughout our American culture and possibly even more so in our global economy. From National Security to Homeland Security to Information Security, we are bombarded with threats everywhere we turn. The Internet reports on new vulnerabilities, carries new viruses and their corresponding definitions, and spreads spy-ware, mal-ware, and bogus e-mail phishing scams every day. There are other vulnerabilities besides viruses, worms, and scams that actually bend the rules of network communication to their benefit. They take advantage of the methods our networks use to transfer data, and these vulnerabilities will always be a threat to our information's security.

Man in the Middle attacks come in many variations and can be carried out on a switched LAN easier than one might think by using tools freely available on the Internet. The following paper will explain how Man in the Middle attacks are possible, the potential threats from such an attack, and finally this paper will demonstrate the use of Cain & Abel to carry out a Man in the Middle attack.

To understand how Man in the Middle attacks can take place we need to look at the way computers communicate. The following paragraph will briefly outline how hosts transfer data on a switched Ethernet LAN.

In the most basic and most common network environment, 802.3 Ethernet, computers communicate at Layer 2 of the Open Systems Interconnection Model using Ethernet frames. Frames are sent to a destination Media Access Control (MAC) address that is unique to each Network Interface Card (NIC) on the network. If the destination MAC address is unknown then the transmitting computer will send an ARP Request (Address Resolution Protocol). An ARP Request is broadcast to every host on the

network. This request asks for the MAC address of a certain IP address that the computer wants to reach. There is a tendency for people to falsely state what ARP does (I have run into this time and again during my research) so I will clarify and state it explicitly here: ARP resolves a MAC address from an IP address (Plummer). Every host on the network receives the ARP Request because it is broadcast but only the host with the corresponding IP address will reply to the request. All of the other computers will process the request and then drop it. The host with the correct IP address uses an ARP Reply that contains its own MAC Address to answer the ARP Request (Sipes). At this point both machines will update their ARP cache that holds the IP address and MAC address mappings of the remote host for a period of time in the ARP cache table. Communication between the hosts can begin after the ARP cache table is created. This table will be used for future data transfer until this information ages out. An illustration of the process is shown in Figure 1 where Host A wants to communicate with Host B.

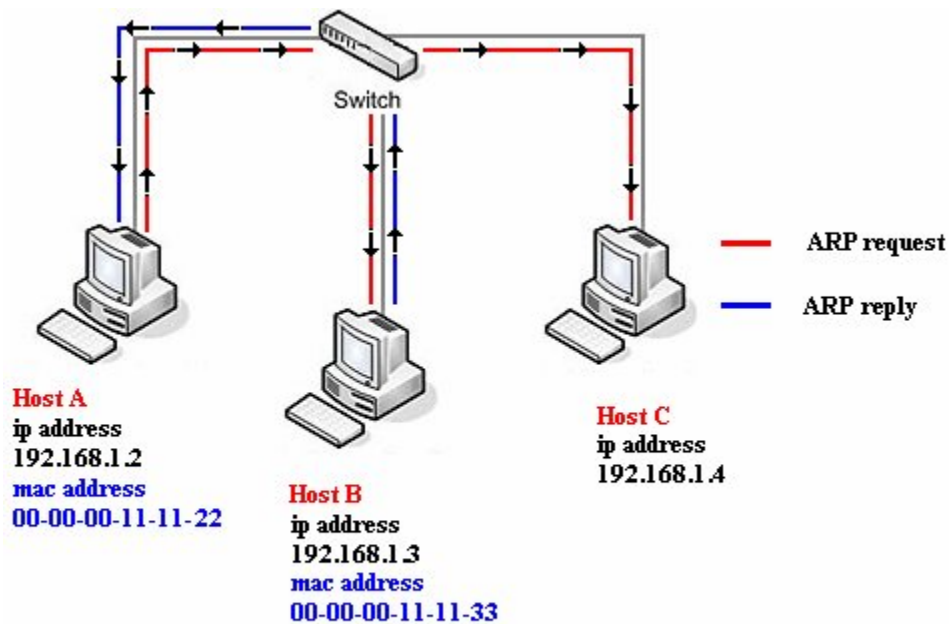
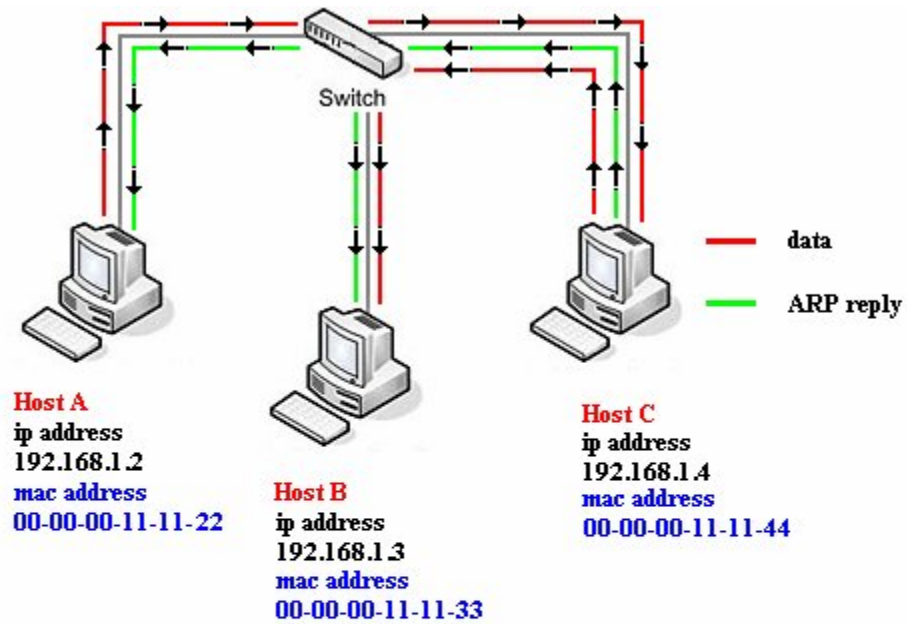


Figure 1

As you can see this communication model relies heavily on trust and assumes that all ARP Reply traffic is legitimate and “playing by the rules”. This is the key to sniffing switched LAN’s and is ultimately what allows Man in the Middle attacks to occur. ARP is a stateless protocol meaning that the computer does not keep track of whether it has sent an ARP Request out (Whalen). Stated another way, when a computer receives an ARP Reply it does not check to see if it has sent an ARP Request. ARP Request/Reply also does not require authentication between the hosts. These two factors allow a computer’s ARP cache to be updated simply by sending an ARP Reply with the wrong MAC address information (Montoro). This vulnerability of spoofing ARP Replies and forcing a target machine to update its ARP cache with incorrect MAC Address information exists within the TCP/IP stack, which means that it is a multi-platform vulnerability. The process of forcing a target machine to update its ARP cache is known as ARP cache poisoning or ARP spoofing. It is important to note that computers create and update the ARP cache dynamically as needed and after a timeout period the contents of the ARP cache will be removed from the table. This is why the computer performing the ARP poisoning must routinely poison each host for the duration of the session (Montoro). An illustration of ARP poisoning is shown in Figure 2.



ARP cache table Host A	
ip address	mac address
192.168.1.3	00-00-00-11-11-44
ARP cache table Host B	
ip address	mac address
192.168.1.2	00-00-00-11-11-44

Figure 2

Now that we understand how computers communicate and how we can fool a device into sending data wherever we want to on the LAN we can start to think about what we can do with this knowledge. ARP poisoning can be used for legitimate purposes such as redirecting new hosts to a network registration page to gain full access to the network. ARP poisoning can also be used for more illicit activities that usually come in the form of Man in the Middle attacks. Man in the Middle attacks have the potential to eavesdrop on a switched LAN to sniff for clear-text data (McClure, Scambray). It can also be used for substitution attacks that can actively manipulate data. Replay attacks can also be used to resend a sniffed password hash to authenticate an unauthorized user. And

finally denial of service attacks can take place during and/or after the Man in the Middle attack is complete (Wagner).

These kinds of attacks can compromise the confidentiality of data and also the integrity of the data as it passes through the local network. As you will see in the following paragraphs any data transmitted in clear-text such as FTP and telnet can easily be stripped out and viewed. Using Cain & Abel version 2.8.8 an individual can easily gather interesting data, mainly usernames and passwords.

The first step is to download, install and run Cain & Abel. This program is provided for free and can be obtained at <http://www.oxid.it/>. While the program is running select “Configure” in the menu bar. This allows you to choose the Ethernet card that you will use to sniff traffic. Select the device and click OK. Cain’s user interface has several tabs located at the top labeled Protected Storage, Network, Sniffer, LSA Secrets, Cracker, Traceroute, CCDU, and Wireless. These features are all interesting and powerful but the majority of them do not concern this particular paper. We are interested in the Sniffer tab of the application. This tab allows us to sniff traffic on the network and select hosts to initiate a Man in the Middle attack.

When you select the Sniffer tab notice that new tabs appear at the bottom of the window that are labeled Hosts, APR, Routing, Passwords, and VoIP. The screen should default to Hosts, if it does not, select the Hosts tab. Next, activate the sniffer by clicking on the icon that looks like a NIC (see Figure 3).

APR-SSH1 can capture and decrypt SSH version 1 sessions that are then saved to a text file. APR-HTTPS can intercept and forge digital certificates on the fly but because a trusted authority does not sign these certificates a warning message will be displayed to the end user. APR-RDP can capture and decrypt Microsoft's Remote Desktop Protocol as well. All of these are basically automated with the exception of APR-DNS where you have to specify which DNS request you would like to redirect. The most crucial item in that list is the radioactive hazard icon labeled APR. It is in this window that we select our victim(s).

Click on APR in the left window pane, then click in the right window pane. Click on the blue plus sign to select the hosts that you would like to put your computer between (see Figure 6).

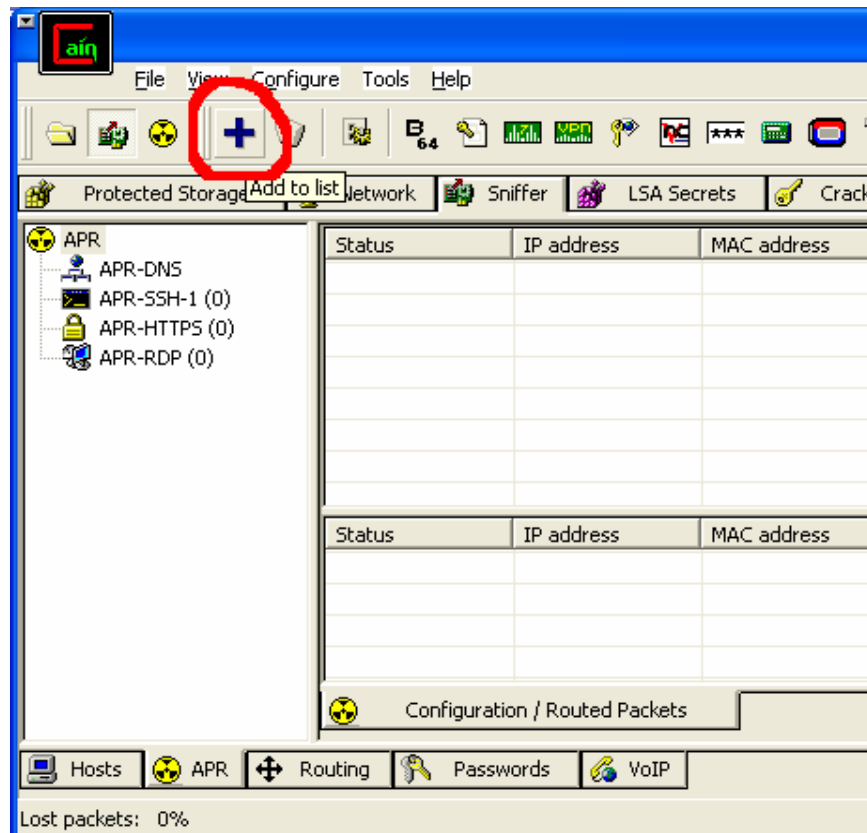


Figure 6

When you select the first host on the left side, the remaining hosts will appear on the right side. You will need to select a host on the right side to continue. If the host you have chosen is a router that has an external link to the Internet, then you will capture all traffic between the host on the internal LAN and the Internet (this tends to be where some very interesting information is exchanged). After you have selected both hosts Cain will display the target host's IP address and the destination host's IP address and what state the connection is in, Idle or Poisoning (see Figure 7).

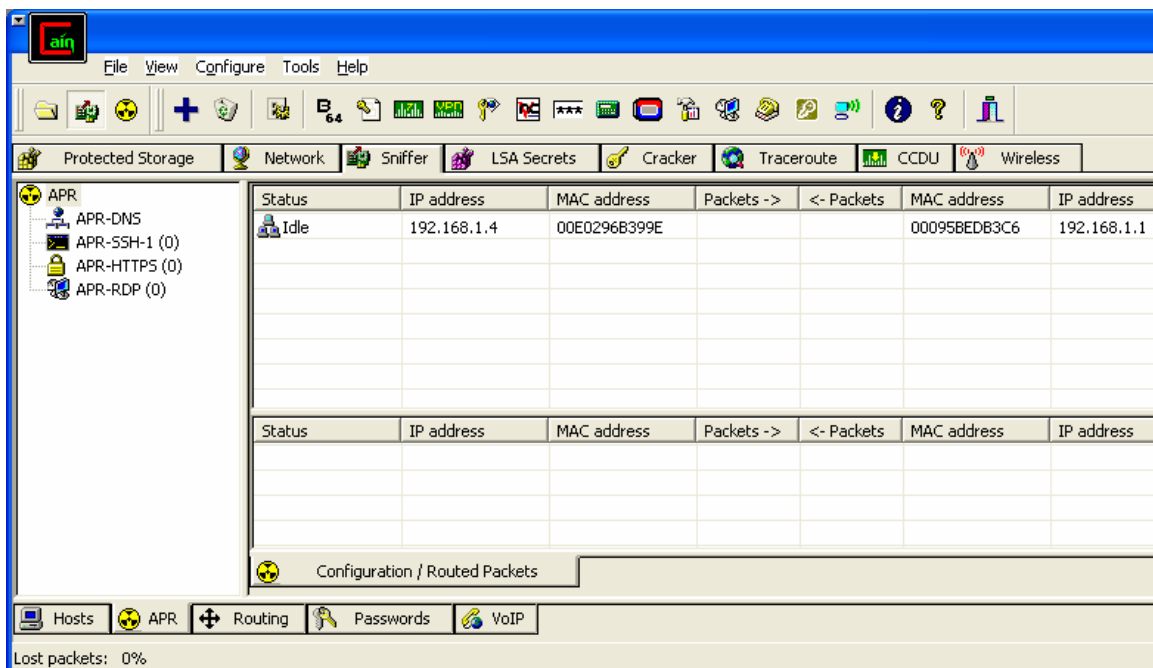


Figure 7

To begin ARP Poisoning, the Man in the Middle attack, simply click on the radioactive hazard symbol next to the NIC Sniffer icon at the top left corner of the window. You are now successfully launching a Man in the Middle attack. To verify that the ARP cache has been poisoned simply log into the remote host and check the ARP cache table by opening the command prompt and then type `arp -a` in the command line interface and you will see the ARP cache table entries (see Figure 8).

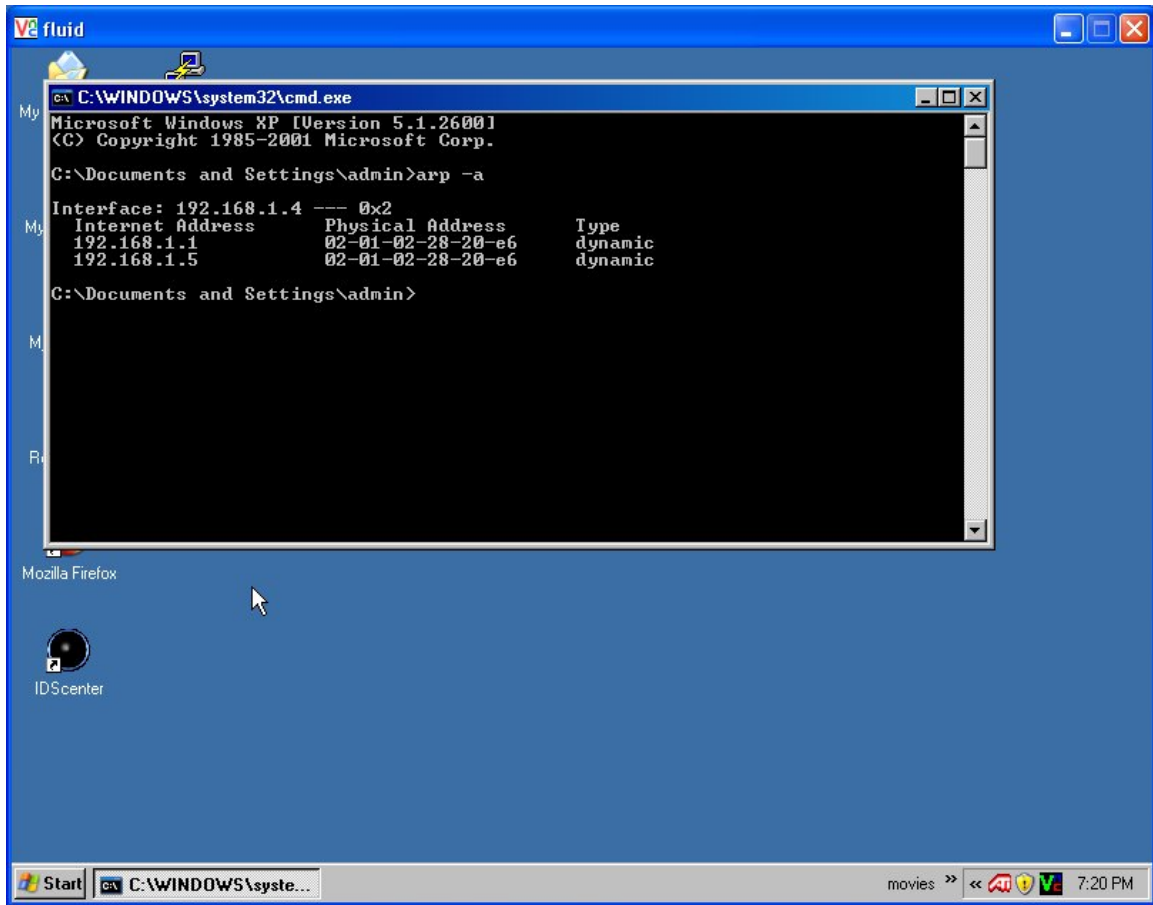


Figure 8

By opening and establishing a telnet session or ftp session to a server on the remote machine you can easily see the danger of clear-text protocols by clicking on the Passwords tab on the bottom of the window (see Figure 9).

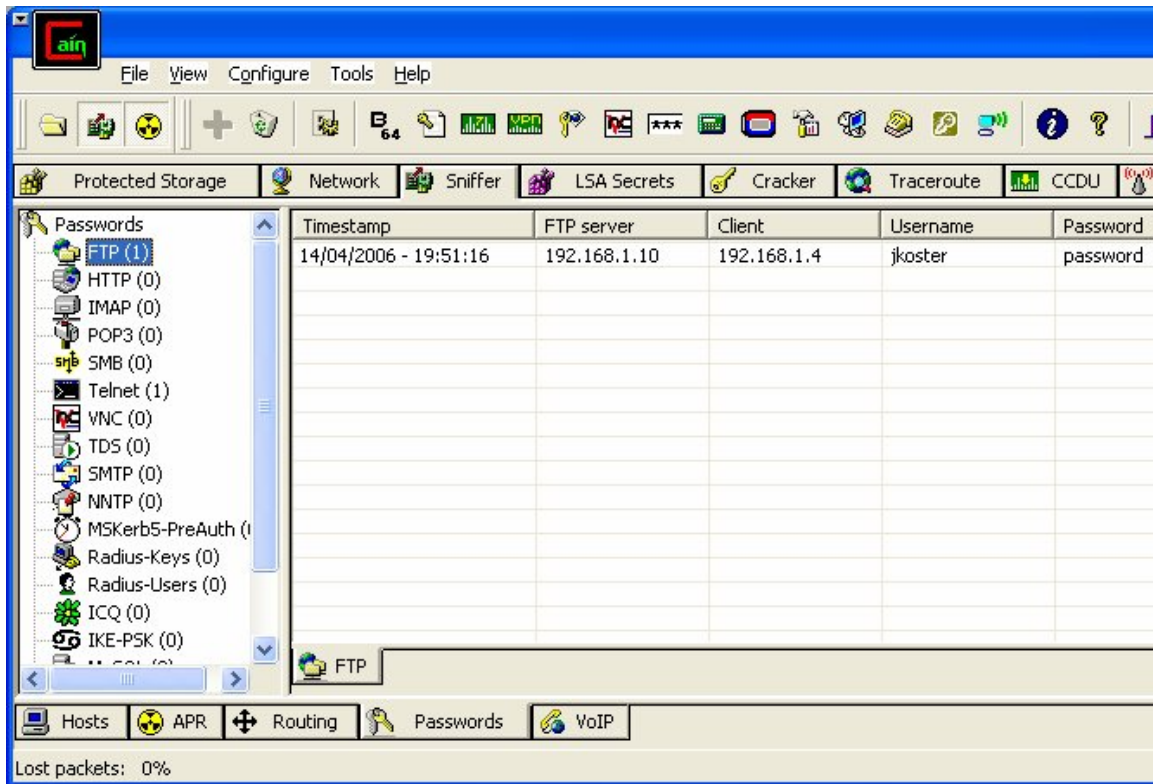


Figure 9

While the Man in the Middle attack is running it might be interesting to see all of the traffic that Cain is processing, for this you can use Ethereal or any other packet capture utility. Ethereal is another free program that is available from <http://www.ethereal.com/>.

Now that you are able to launch successful Man in the Middle attacks and sniff traffic on your switched LAN it is important to remember to use your power only for good and only on networks that you have permission to do so on. If you do not heed this warning you may put yourself in a position that you don't want to be in, both ethically and legally. Every person that deals with technology, from a Technical Analyst to a Chief Information Security Officer, should know what he or she is facing, and ARP cache poisoning is only one of many threats to be concerned with. It is our responsibility to secure our networks and enforce policies and procedures that serve the greater good.

References

- McClure, S., Scambray, J. (May 2000) *Switched networks lose their security due to packet-capturing tool*. Retrieved April 13, 2006, from <http://www.infoworld.com/articles/op/xml/00/05/29/000529opswatch.html>
- Montoro, Massimiliano. (June 2001). *Introduction to Arp Poison Routing*. Retrieved April 6, 2006, from <http://www.oxid.it/downloads/apr-intro.swf>
- Plummer, David C. (November 1982). *An Ethernet Address Resolution Protocol*. Retrieved April 11, 2006, from <http://www.ietf.org/rfc/rfc826.txt>
- *Sipes, Stephen. (September 2000). *Why your switched network isn't secure*. Retrieved April 13, 2006, from http://www.sans.org/resources/idfaq/switched_network.php
- *Wagner, Robert. (August 2001). *Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks*. Retrieved April 11, 2006, from <http://www.sans.org/rr/whitepapers/threats/474.php>
- Whalen, Sean. (April 2001). *An Introduction to Arp Spoofing*. Retrieved April 14, 2006, from http://packetstormsecurity.org/papers/protocols/intro_to_arp_spoofing.pdf