

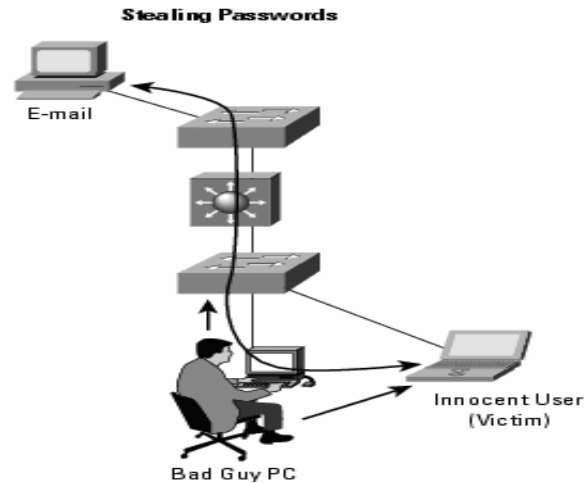


The OSI Model is based upon 7 layers (Application layer, Presentation Layer, Session Layer, Transport Layer, Network Layer, Data Link Layer and the Physical layer). For our purposes we will review layer 2 (data link layer), Data Link layer defines the format of data on the network. A network data frame, aka packet, includes checksum, source and destination address, and data. The data link layer handles the physical and logical connections to the packet's destination, using a network interface. A host connected to an Ethernet network would have an Ethernet interface (NIC) to handle connections to the outside world, and a loop back interface to send packets to itself. Ethernet addressing uses a unique, 48-bit address called its Ethernet address or Media Access Control (MAC) address. MAC addresses are usually represented as six colon-separated pairs of hex digits, e.g., 8A:0B:20:11:AC:85. This number is unique and is associated with a particular Ethernet device. The data link layer's protocol-specific header specifies the MAC address of the packet's source and destination. When a packet is sent to all hosts (broadcast), a special MAC address (ff:ff:ff:ff:ff:ff) is used. Now with this concept covered we need to explain what ARP is and how it corresponds to the MAC address. The Address Resolution Protocol is used to dynamically discover the mapping between a layer 3 (protocol) and a layer 2 (hardware) address. ARP is used to dynamically build and maintain a mapping database between link local layer 2 addresses and layer 3 addresses. In the common case this table is for mapping Ethernet to IP addresses. This database is called the ARP Table. The ARP Table is the true source when it comes to routing traffic on a Switch (layer 2 device).

| <b>IP Address</b> | <b>Hardware Address</b> |
|-------------------|-------------------------|
| 197.15.3.2        | 0A:07:4B:12:82:36       |
| 197.15.3.3        | 0A:9C:28:71:32:8D       |
| 197.15.3.4        | 0A:11:C3:68:01:99       |
| 197.15.3.5        | 0A:74:59:32:CC:1F       |
| 197.15.3.6        | 0A:04:BC:00:03:28       |
| 197.15.3.7        | 0A:77:81:0E:52:FA       |

**ARP Table**

Now that we have explored MAC addresses and ARP Tables we need to talk about poisoning. ARP Poisoning; also referred to as ARP poison routing (APR), ARP cache poisoning, & spoofing. A method of attacking an Ethernet LAN by updating the target computer's ARP cache/table with both a forged ARP request and reply packets in an effort to change the Layer 2 Ethernet MAC address (i.e., the address of the network card) to one that the attacker can monitor.



Because the ARP replies have been forged, the target computer sends frames that were meant for the original destination to the attacker's computer first so the frames can be read. A successful APR attempt is invisible to the user. Since the end user never sees the ARP poisoning they will surf online like normal while the attacker is collecting data from the session. The data collected can be passwords to e-mail, banking accounts, or websites. This kind of attack is also known as "Man in the Middle Attack". This kind of attack basically works like this: attackers PC sends poisoned ARP request to the gateway device (router), The gateway device now thinks the route to any PC on the subnet needs to go though the attackers PC. All hosts on the subnet thinks the attackers IP/MAC is the gateway and they send all traffic though that computer and the attacking PC forwards the data to the gateway. So what you end up having is one PC (attacker) sees all traffic on the network. If this attach is aimed at one user the Attack can just spoof the victims MAC to his own and only affect that MAC on the subnet. Keep in mind that the gateway (router) is designed to have lager routing tables and many sessions connected to it at once. Most PC's can not handle too many routes and sessions so the attackers PC has to be a fast PC (this depends on the volume of traffic on the subnet) to keep up with the flow of data. In some cases a network can crash or freeze if the attacker's PC is unable to route the data effectively. The network Crashes because the number packets dropping due to the fact the Attackers PC is unable to keep up with the flow of data.



### **Wardriving Anyone?**

Now a lot of people think there safe because there home network is inside there house. Well this is not true you first should always have a firewall on any internet connection. An attacker can just as easy spoof the ISP's devices (Cable modem or DLS router) to get all your out bound data. If you are using wireless remember to setup encryption or you have just invited Attackers into you home with no firewall to block them. I have drove in many cities with my wireless card on seeing over 60% of all AP's open with no security. There is a sport called Wardriving witch involves driving in your car with a wireless network card to find wireless networks. Most Wardrivers do not get onto the networks they find but they do document them (normally with GPS). The idea behind Wardriving is just to see how many AP's you can find and this sport has caught on big in the US. It would be very easy to get an IP on a Wireless network and then ARP Poison the subnet. This can be done in less than 2 minutes on an open wireless access point. Once the attacker is on your subnet they can start receiving all your data so if you buy anything online the attacker now has you credit card info. There are ways to prevent this kind of attack but most switches are vulnerable to this kind of attack. To prevent ARP Poisoning you need a Switch that supports security features and most vendors' equipment can handle this but theses kinds of switch devices normally cost more money. Keep in mind that there are many free tools on the internet that perform ARP Poisoning/Spoofing. It is not hard to use the tools and with more and more home users going wireless the risk of an attacker getting you data keeps rising. The best thing to do for protection is to understand the basics of your network and if you want wireless make sure you have WEP enabled.



### **The Good Guys**

So far we have covered how attackers use ARP Poisoning to intercept user's data but there are also good reasons to ARP Poison a network. Most network engineers need to sniff the protocols on a network to make sure the data is flowing correct. The problem with sniffing on a switch network is that you can only see data bound to your interface and broadcast traffic. On unmanageable switches there is no way to see all host traffic to inspect it. With ARP Poisoning you can now divert all traffic to pass through the sniffer's interface and see all data on the network and analyze the traffic for possible issues. Admins & Engineers maybe trouble shooting speed issues on a subnet and need to see all the traffic. Once you spoof the subnet to sniff the traffic you will be able to see if viruses or a bad NIC card is causing a broadcast storm on the subnet. With any tool there are always good and bad uses and the thing to remember is be careful of what you do online because anyone could be monitoring you. If you have any question about poisoning feel free to send me an e-mail at [slimjim100@gmail.com](mailto:slimjim100@gmail.com).