

Pick Your Poison - ARP, MAC, WiFi

del.icio.us

Discuss in Forums {mos_smf_discuss:Wilson}

By Brian Wilson, CCNA, CCSE, CCAI, MCP, Network+, Security+, JNCIA

In this paper we will cover the basics on Address Resolution Protocol (ARP), Media Access Control (MAC) Addresses, Wireless (WiFi), and layer 2 communications. I hope to explain how a "Man in the Middle Attack" works. The common name for this is ARP poisoning, MAC poisoning, or Spoofing. Before we can get into how the poisoning works, we need to learn about how the OSI Model works and what happens at layer 2 of the OSI Model. To keep this basic we will only scratch the surface on the OSI model to get the idea of how protocols work and communicate with each other. The OSI (Open Systems Interconnection) Model was developed by the International Standards Organization (ISO) in 1984 in an attempt to provide some standard to the way networking should work. It is a theoretical layered model in which the notion of networking is divided into several layers, each of which defines specific functions and/or features. However this model is only a general guideline for developing usable network interfaces and protocols. Sometimes it may become very difficult to distinguish between each layer as some vendors do not adhere to the model completely. Despite all this the OSI model has earned the honor of being "the model" upon which all good network protocols are based.

The OSI Model

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). The Data Link layer defines the format of data on the network. A network data frame, aka packet, includes checksum, source and destination addresses, 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 a Network Interface Card (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 to all Ethernet devices. 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 Address Resolution Protocol (ARP) is and how it corresponds to the MAC address. The ARP 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).

ARP Table

Now that we have explored MAC addresses and ARP Tables, we need to talk about poisoning. ARP Poisoning is also referred to as ARP poison routing (APR), ARP cache poisoning & spoofing. A method of attacking an Ethernet LAN is by updating the target computer's ARP cache/table with both a forged ARP request and reply packets. This is done 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. Packets are routed via the ARP Table through the Attacker's computer.

The Attack

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:

1. Attacker's PC sends poisoned ARP request to the gateway device (router)
2. The gateway device now thinks the route to any PC on the subnet needs to go through the attacker's PC.
3. All hosts on the subnet think the attacker's IP/MAC is the gateway and they send all traffic through that computer.
4. 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 attack is aimed at one user, the

attacker 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 larger routing tables and many sessions connected to it at once. Most PCs can not handle too many routes and sessions, so the attacker's PC has to be fast (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 attacker's PC is unable to keep up with the flow of data.

Wardriving Anyone?

Now a lot of people think they're safe, because their home network is inside their house. Well this is not true! First things first, you should always have a firewall on any internet connection. An attacker can just as easily spoof the ISP's devices (Cable modem or DSL router) to get all your outbound data. If you are using wireless, remember to setup encryption, otherwise you have just invited attackers into your home with no firewall to block them. I have driven in many cities with my wireless card on and saw over 60% of all APs unsecured. There is a sport called Wardriving that involves driving in your car with a wireless network card to find available networks. Most Wardrivers do not connect to the networks they find, but they do document them (normally with GPS). The idea behind Wardriving is just to see how many APs 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 of your data, so, if you buy anything online, the attacker now has you credit card information. There are ways to prevent this kind of attack, but most switches are vulnerable. To prevent ARP Poisoning you need a switch that supports security features, and most vendors' equipment can handle this. On the other hand, these 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 your 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 (Network Engineers)

So far we have covered how attackers use APR 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 correctly. The problem with sniffing on a switched network is that you can only see data bound to your interface and broadcast traffic. On unmanaged 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 sniffers interface and see all data on the network. Now the good guys can analyze the traffic for possible issues. Admins & Engineers may be troubleshooting 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. 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.

Brian Wilson (bwilson@ethicalhacker.net) has over 12 years experience in IT starting with a tour in the United States Army. He has worked in and out of the US Government in many different organizations and technical roles including a stint as a Cisco Certified Instructor. Currently he works for one of the largest US broadband providers (ISP) as a Senior Data/Voice Engineer supporting over 3 million High Speed Internet/ VoIP subscribers. He has attained a number of industry credentials covering many aspects of IT including CCNA, CCSE, CCAI, MCP, JNCIA, Network+, Security+, and many DoD Certifications. He also uses his knowledge of IT to benefit a number of charitable organizations. Clearly Brian's

knowledge and interests are wide, and his affinity for philanthropy will be the overriding theme of his vast set of articles and videos.