Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks

The classic Man-in-the-Middle attack relies upon convincing two hosts that the computer in the middle is the other host. This can be accomplished with a domain name spoof if the system is using DNS to identify the other host or address resolution protocol (ARP) spoofing on the LAN. This paper is designed to introduce and explain ARP spoofing. The term Man-in-the-Middle is used from a historical usage, this does not imply that only men can use these attacks. Perhaps Teenager-in-the-Middle or Monkey-in-the-Middle may be ...

Copyright SANS Institute
Author Retains Full Rights

AD

Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks

Practical Assignment GSEC Version 1.2f (amended August 13, 2001), ***Robert Wagner***
Updated June 2006 ***Jeff Bryner****, CISSP,GCIH-Gold, GCFA-Gold*

Abstract

The classic Man-in-the-Middle attack relies on convincing two hosts that the computer in the middle is the other host. This can be accomplished with a domain name spoof if the system is using DNS to identify the other host or address resolution protocol (ARP) spoofing on the LAN.

This paper is designed to introduce and explain ARP spoofing and its role in Man-in-the-Middle attacks. The term Man-in-the-Middle is historical usage -- it does not imply that only men can use these attacks. Perhaps Teenager-in-the-Middle or Monkey-in-the-Middle would be more accurate terms.

Ethernet Is Not Just for IP

Most networks today are Ethernet networks using TCP/IP for communications. This marriage between IP and Ethernet networking is so common that most people don't even think about the traffic happening at the Ethernet layer of the network. IP is often viewed as the sole means of routing a packet. But once an IP packet comes into an Ethernet Local Area Network (LAN), it must be converted into a packet that Ethernet can understand. Ethernet was built to support protocols other than just TCP/IP and therefore does not rely on IP addresses to deliver packets. When an Ethernet device delivers an IP packet to a network segment, the packet is encapsulated into an Ethernet frame for local handling. This frame uses the network card's hardware address when transmitting packets between systems.

This hardware address is referred to as the Media Access Control (MAC) address. MAC addresses are a 48 bit number, and are to be unique in their identification of a particular piece of equipment. The address is written as 6-byte hex strings such as 00:0B:CD:B3:38:B3, with colons separating the bytes. When an Ethernet interface receives a packet, it looks at the MAC address to see if the packet is destined for it. If so, it picks it up off the wire and passes it up the operating system (OS) layers to be further processed.

When sending an IP packet, Ethernet uses the Address Resolution Protocol (ARP) to resolve IP addresses into hardware MAC addresses. Once the destination's MAC address is determined, the IP Packet can be encapsulated into an Ethernet frame and transmitted to the destination host.

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

ARP

Address Resolution Protocol is defined mainly by RFC 826 http://www.faqs.org/rfcs/rfc826.html. Within Ethernet ARP, there are four types of messages.

> ARP request: A request for the destination hardware address that is typically sent to all hosts.
> ARP reply: In response, this gives the host the hardware address of the destination host.
> RARP request: Known as Reverse ARP request, this requests the IP address of a known MAC address.
> RARP reply: The response gives the IP address from a requested hardware address.

ARPs Role in Ethernet Switching and Sniffing

Since Ethernet is a broadcast protocol, everyone on an Ethernet segment receives everyone else's packets. On a network connected with a hub, sniffing packets to gather information is easy since hubs do nothing to limit the natural broadcast nature of Ethernet. Sniffing data is as easy as plugging into any open port and listening. Systems connected with switches present a different problem. Traffic is no longer broadcast to every host as the switch attempts to be more efficient. Instead the switch keeps track of what MAC address is at what port and makes an attempt to limit traffic based on this information. This is not meant to be a security feature, but rather a performance feature.

To keep down the ARP traffic on a network segment, Ethernet hosts and switches keep an ARP cache usually consisting of a list of MAC and IP addresses. The system will use this information when initiating a conversation with another system. If the address is not in the table, the system will use ARP to determine the MAC address of the destination system. Switches use ARP tables to limit the traffic that a port receives to just the MAC address registered for that port.

In switched environments, there are still ways to sniff packets. The first is to connect to an administrative port on the switch and set it to broadcast mode. The administrative port will now receive all traffic. Some switches allow one to choose the administrative port in a software setup, while others restrict it to one particular physical port.

The second method is to take advantage of the fact that most switches will favor performance over security and quit using the internal cache of MAC to IP address table if the table becomes too large. The switch will usually fail-open and revert to hub-like behavior, sending all packets to everyone. An attacker can initiate a fail-open by sending a large number of ARP entries to the switch. This behavior varies depending upon the manufacturer and switch configuration.

The final method is to craft ARP packets to fool a system into thinking it knows the MAC address of a particular destination IP address. Most commonly an attacker will impersonate a router by telling a victim that the attacker's machine is the default router for a subnet. The victim's system then sends all packets to the attacker who sniffs them and sends them on to the real default router either through kernel level IP forwarding or a user space program.

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

Other ARP attacks include sending bogus ARP entries to cause a denial of service as the victim machine sends packets to the wrong address. An attacker can also take over a victim's MAC and IP address and then impersonate the victim in network conversations.

ARP Manipulation

The remainder of this paper will examine several tools and methods for gathering, manipulating and defending ARP information. First one should know where to find ARP information on a system. On most systems the 'arp' command allows one to list and manipulate the local system ARP table. ARP –a will usually list the entries currently in the arp table. On some systems, arp –an can be used to avoid having the local system look up the DNS name of the systems in the list. The resulting list usually consists of the IP address, the MAC address and the Ethernet interface. The MAC address for a system can be found by logging on to that system and using ifconfig on unix, or ipconfig on windows.

Operating Systems vary in how they treat the ARP table and ARP packets in general. Some systems will accept gratuitous ARP packets and gladly insert the information into their table. Some systems will not accept an entry if they already have the information in their table. Some systems wait until entries have timed out before accepting updates. Some systems will not accept an entry unless they have asked for it. Even in systems that protect the ARP table, approaches such as sending a spoofed ping over ICMP containing the desired MAC/IP information can be effective.

Now let's look at some tools that can be used in ARP attacks. Please note that these tools are not meant for production networks and can easily lead to unintended consequences. Please examine these tools with caution.

Arpoison http://arpoison.sourceforge.net/

Arpoison is a simple command line tool by Steve Buer that creates a custom ARP Reply packet.

The attacker simply creates a packet, sends it to the victim and hopes the victim system inserts the information into its local ARP table and acts on it when sending future packets.

From the main page for arpoison:

```
NAME
       arpoison -- arp cache update utility

SYNOPSIS
       arpoison -i <device> -d <destIP> -s <sourceIP> -t <targMAC> -r
<srcMAC> [-a] [-n number of packets] [-w time between packets]

DESCRIPTION
       Arpoison constructs an ARP REQUEST or REPLY packet using the
specified hardware and protocol addresses and sends it out the
specified interface.


       -i     Device e.g. eth0
```


© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

```
-d      Destination IP address in dotted decimal notation.

-s      Source IP address in dotted decimal notation

-t      Target MAC address e.g. 00:f3:b2:23:17:f5

-r      Source MAC address

-a      Send ARP REQUEST

-n      Number of packets to send

-w      Time in seconds between packets
```

If you have physical access, MAC addresses for the target systems can be found using ifconfig on UNIX and ipconfig on Windows. Otherwise a simple ping from the LAN segment of the victim will return the MAC address as part of the packet. Sniff the packet using tcpdump or some other utility and you have your MAC information. Additionally the MAC address of ff:ff:ff:ff:ff:ff can be used to broadcast to all hosts on the local network segment.

At the time of this writing, the following test results were observed when sending bogus ARP reply packets to these operating systems:

Windows 2000 Service Pack 4 accepted ARP packets.
Windows XP Professional Service Pack 2 refused the ARP packets.
Gentoo Linux 2.6.14-gentoo-r5 refused the ARP packets.

Systems are reported as accepting the ARP packets if they displayed the bogus ARP information sent during the test in their ARP tables.

Ettercap http://ettercap.sourceforge.net/

Ettercap is an enhanced sniffer for Unix-based systems. The software allows the user to collect data and/or passwords from a variety of protocols including TELNET, FTP, POP, RLOGIN, SSH1, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, HALF LIFE, QUAKE 3, MSN, YMSG, etc..

The program allows the user to poison the ARP cache on systems, and by doing so, sniff switched LANs and become the default router for a victim. Once this has been accomplished, acting as a Man-in-the-Middle is an easy act. Because packets are being sent through the attacker's computer, injecting malicious commands into an existing session is automated through this software. Once in the middle of conversations, the attacker also has the ability to drop packets. This is particularly problematic with protocols such as Syslog over UDP where the session may not be expecting the packet and lost packets do not raise an alarm.

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

Parasite: http://packetstormsecurity.org/groups/thc/parasite-1.2.tar.gz

Parasite is a tool with the ability to perform ARP spoofing, MAC flooding and MAC duplicating. In spoofing mode, instead of just sending out blind ARP replies, it waits until it sees ARP requests, and then replies, which increases the chance that the ARP spoofing attack will be successful. "parasite -F eth0" initiates a MAC flood which attempts to overrun the memory allocation for MAC addresses inside a switch, forcing it to act as a hub and send all packets to everyone. "parasite -m <mac address> eth0" initiates a MAC duplication attack so the attacker can impersonate a victim or cause denial of service.

Dsniff http://monkey.org/~dugsong/dsniff/

The final tool profiled here is Dsniff. This tool provides password sniffing and Man-in-the-Middle attacks for SSH and SSL. The tool can intercept passwords for telnet, FTP, SMTP, HTTP, POP, IMAP, LDAP, Rlogin, RIP, OSPF, PPTP, MS-CHAP, NFS, VRRP, etc.

At the ARP level, Dsniff provides a tool called arpspoof to inject gratuitous ARPs onto the wire, and macof to flood a switch in the hopes of turning it into a hub.

As an auditing tool, it can be used to see if these protocols are in use on a network and if the network in general is vulnerable to attack. Similar to Ettercap, this program can use ARP or DNS poisoning to trick a host into communicating through it. Both the HTTPS and SSH Man-in-the-Middle attacks are performed through DNS poisoning, which allows the attack to occur outside a LAN subnet.

Ettercap and Dsniff both illustrate the increasing ease of pulling off a sophisticated attack like Man-in-the-Middle. Tools like these effectively illustrate the trend towards making once theoretical attacks just a click away.

Defending Against ARP Attacks

Preparation

The best defense is to know thy system. If your network is static or has few changes, then it makes sense to include MAC/ARP information in the network design and documentation. A small DMZ with limited servers should have a fairly static ARP/MAC footprint, and alarms should set off if a new MAC address is visible within the subnet, or is mapped to a differing IP address. Keep in mind that most IDS systems do little to monitor or alert on suspicious ARP traffic. Even SNORT lists ARP as a protocol they intend to monitor in the future. Additionally, monitoring a network for ARP/MAC changes will have its own share of false positives as network cards are swapped out, or dual NIC configurations change, etc.

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

Host Hardening

ARP tables on systems can be statically mapped usually using the arp -s command. However, different versions of operating systems have different respect for this static mapping. Even with a static mapping, some systems have been reported to accept gratuitous ARPs and overwrite the static mapping. Some systems will allow ARP to be completely removed from the Ethernet interface and rely solely on static ARP tables. Static mapping should be tested with your target OS for durability during ARP attacks. Inventory your network host operating systems for their response to ARP attacks so you know what your network is vulnerable to.

Switch Hardening

Like many switches, Cisco's IOS offers protection against ARP attacks. IOS has a command called: Set Port Security. Enabling this feature will restrict the switch such that only one (default) MAC address is allowed per physical port. This command allows one to configure the action that will take place upon a hardware address change. By limiting the number of hardware addresses per port to one, a host cannot change his hardware address on the fly or try to map multiple MAC addresses to route traffic out one port. This will not analyze the MAC/IP table and take action during changes. It will not have any affect on DNS spoofing. An attacker could use this as a denial of service tool by forcing hardware address changes on a host.

Identification

ARP attacks are difficult to discover. They can appear as ephemeral network disturbances, or widespread denial of service. Access to a particular system's ARP information is usually only available by logging into the system and querying the ARP cache. Operating systems are usually quiet about their ARP cache and do nothing to report on changes within it, suspicious or not. Network sniffers can help pinpoint ARP shenanigans, but often require much filtering to get useful data.

ARPWATCH http://www-nrg.ee.lbl.gov/

Arpwatch contains functionality designed to monitor the IP/MAC table and record changes via syslog and email. This is a very simple and straightforward piece of software that can be easily run on any Linux system. Here are some samples of what will show up in the /var/log/messages file.

```
Sep 20 12:36:11 myhost arpwatch: new station 192.168.a.b 0:50:94:d7:ca:d5
Sep 20 12:35:07 myhost arpwatch: changed ethernet address 192.168.a.c 0:10:a4:bf:b1:c9 (0:0:86:45:32:fa)
```

The first line shows a new IP/MAC address combination. This will appear every time arpwatch has discovered a new host on the LAN subnet. The second line shows that the MAC address has changed for host 192.168.a.c. The new MAC address is 0:10:a4:bf:b1:c9. The previous address was 0:0:86:45:32:fa. This should cause the system administrator to pause and review some basic information about the host. If this is a dedicated server, then the address shouldn't change without switching the hardware. If it's an address space assigned to DHCP as one host leaves the network and a separate host picks up its IP address, this change may be appropriate. Please note, by using the

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

hardware address to identify the vendor, one may notice that the changed MAC address changed from a Xircom to Gateway Communications (bought by Megahertz and then 3Com). This could also alert one to hardware that is outside of their LAN inventory.

Containment

If you discover signs of ARP spoofing or switch table flooding, keep an eye out for the tools mentioned above. Keep in mind that warnings from tools like arpwatch can also be triggered by NIC card replacements, failing NIC teaming drivers, DHCP misconfiguration, etc. It can be challenging to trace the source of an ARP attack, since the MAC/IP address used in the attack is likely to be the same as a valid host on the network. If tracking down 'New Station' alerts, the MAC address can sometimes be helpful in determining the manufacturer of the NIC card as MAC addresses are tied to vendors. For example a 'new station' alert on a Cisco MAC Address is likely the addition of a router or wireless access point.

Switches, routers and other network devices can help keep the problem from getting worse. If you suspect ARP hooligans, you can enable port security, and dump the ARP tables of nearby routers and switches to determine where the tables differ or overlap.

Eradication

If you are able to find a rogue host or a rogue sniffer program installed on a valid host, follow your incident response procedures in collecting evidence about the host or program. Everything about the host/program could become important later, so be sure to document everything possible. If removing a sniffer program, be sure to check that the network interfaces on the machine have returned to a non-promiscuous mode. Also be sure that gratuitous ARP entries have been cleared from all hosts on the affected subnet.

Recovery

Be sure to monitor the affected subnet and hosts closely for further suspicious ARP behavior. You may want to tighten switch port security settings, reset arpwatch cache data, clear neighbor ARP caches, etc.

Summary

Ethernet has become almost synonymous with TCP/IP in most networks. Yet its role in network traffic is often overlooked or misunderstood. ARP attacks remind the security professional that the simple attacks are often the most successful. With the right tools, simple ARP spoofing can become the building block for much more sophisticated attacks against advanced security measures like SSL, SSH, etc. When auditing, designing or defending your next network, be sure to give a thought to the role of ARP in that network.

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

References and Further Information

Watson, Keith and Noordergraaf, Alex. Solaris Operating Environment Network Settings for Security (December 2000) http://www.sun.com/blueprints/1200/network-updt1.pdf

Fermilab. Data Communications and Networking Group. How to find your MAC address (05 February 2001) http://www-dcn.fnal.gov/DCG-Docs/mac/

Roesch, Martin Snort Users Manual, Snort Release: 2.0.0 (8 April 2003) http://www.snort.org/docs/SnortUsersManual.pdf

Institute 2001. Whalen, Sean. An Introduction to ARP Spoofing (April, 2001) http://packetstormsecurity.org/papers/protocols/intro_to_arp_spoofing.pdf

Fairhurst, Gorry. Address Resolution Protocol (arp) (01 January 2001) http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html

Ethernet Codes Master Page (26 October 1998)
Used to match MAC address to hardware vendor.
http://www.cavebear.com/CaveBear/Ethernet/

Cisco. IOS Commands. Set Port Security
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_5_4/cmd_ref/set_po_r.htm#xtocid573819

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

Last Updated: August 27th, 2011

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Melbourne 2011	**Melbourne, Australia**	**Sep 05, 2011 - Sep 10, 2011**	**Live Event**
SANS Delhi 2011	**Delhi, India**	**Sep 12, 2011 - Sep 17, 2011**	**Live Event**
SANS Network Security 2011	**Las Vegas, NV**	**Sep 17, 2011 - Sep 26, 2011**	**Live Event**
2011 European Digital Forensics and Incident Response Summit	**London, United Kingdom**	**Sep 21, 2011 - Sep 27, 2011**	**Live Event**
SANS SEC401 with FIS Saudi Arabia 2011	**Riyadh, Saudi Arabia**	**Sep 24, 2011 - Sep 29, 2011**	**Live Event**
Security Architecture 2011	**Washington, DC**	**Sep 29, 2011 - Sep 30, 2011**	**Live Event**
SANS Gulf Region 2011	**Dubai, United Arab Emirates**	**Oct 08, 2011 - Oct 22, 2011**	**Live Event**
SANS Baltimore 2011	**Baltimore, MD**	**Oct 09, 2011 - Oct 15, 2011**	**Live Event**
SOS: SANS October Singapore 2011	**Singapore, Singapore**	**Oct 10, 2011 - Oct 18, 2011**	**Live Event**
National Cybersecurity Innovation Conference	**Washington, DC**	**Oct 11, 2011 - Oct 14, 2011**	**Live Event**
Grid SecCon 2011	**New Orleans, LA**	**Oct 18, 2011 - Oct 18, 2011**	**Live Event**
SANS Chicago 2011	**Chicago, IL**	**Oct 23, 2011 - Oct 28, 2011**	**Live Event**
SANS Seattle 2011	**Seattle, WA**	**Nov 02, 2011 - Nov 07, 2011**	**Live Event**
SANS FOR508 With FIS Abu Dhabi 2011	**Abu Dhabi, United Arab Emirates**	**Nov 05, 2011 - Nov 10, 2011**	**Live Event**
SANS Korea 2011	**Seoul, Korea, Republic Of**	**Nov 07, 2011 - Nov 12, 2011**	**Live Event**
SANS Sydney 2011	**Sydney, Australia**	**Nov 11, 2011 - Nov 19, 2011**	**Live Event**
SANS Tokyo Autumn 2011	**Tokyo, Japan**	**Nov 14, 2011 - Nov 19, 2011**	**Live Event**
SANS San Francisco 2011	**San Francisco, CA**	**Nov 14, 2011 - Nov 19, 2011**	**Live Event**
SANS SEC566 with FIS Oman 2011	**Muscat, Oman**	**Nov 19, 2011 - Nov 23, 2011**	**Live Event**
European SCADA and Process Control System Security Summit 2011	**Rome, Italy**	**Nov 26, 2011 - Dec 04, 2011**	**Live Event**
SANS Ottawa 2011	**OnlineON**	**Aug 28, 2011 - Sep 02, 2011**	**Live Event**
SANS OnDemand	**Books & MP3s Only**	**Anytime**	**Self Paced**