

RE: ARP Spoofing and Routing

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-10/0017.html>

From: Payton, Zack (Zack.Payton_at_MWAA.com)

Date: 10/01/05

Date: Sat, 1 Oct 2005 14:56:12 -0400

To: "Kyle Starkey" <kstarkey@siegeworks.com>, <pen-test@securityfocus.com>

Kyle,

It sounds to me like you were only doing one way arp spoofing... Meaning that you'd intercepted all arp requests that want to know the mac address of your server. But you have not intercepted all the arp requests sent out from that server. So in otherwords you are only partially performing a Man In The Middle attack. You don't have control over the traffic in both directions. There are some nice tools to automate this process in it's entirety the most complete of which is ettercap. Altering traffic as it flows through your system is fairly trivial. See netsec or iptables MANGLE chain.

Etercap also has some native packet altering capabilities. There's some perl project out there I was reading about that also was designed for this purpose.

Zack Payton

-----Original Message-----

From: Kyle Starkey [<mailto:kstarkey@siegeworks.com>]

Sent: Friday, September 30, 2005 2:33 PM

To: pen-test@securityfocus.com

Subject: ARP Spoofing and Routing

Folks..

I was on site yesterday at a client doing some pen-test type work and thought I might play around with some arpspoofing and see what I could gather. I ran into a couple of problem and thought you all might have the solution.

What I was trying to do was arpspoof a server so that I could intercept any authentication requests that were made to it and grab passwds or hashes to find some user accts. I was using the Auditors Toolkit bootable CD and the arpspoof worked great. A tcpdump of the eth0 int when the spoof started showed that I was getting all the traffic that should have been destined for this server (hosts and server and myself were all in the same bcast seg btw). However I was not running any deamons (ftp, samba, telnet, etc) to answer these requests and as such

SecurityFocus Penetration: RE: ARP Spoofing and Routing

was only seeing part of the conversation and couldn't complete the connection to get the full auth request. So what I need to know is how I go about sending packets that were destined for the server originally to the actual server after I have had my tcpdump/dsniff/etc doing the packet capture and filter. My ideas are as follows and I could use some responses about them or OTHER ways I can accomplish this...

- 1) routed routing traffic to the original host with a static ARP entry in my host for the server I am spoofing so I don't spoof myself
- 2) some kind of proxy server that will capture and forward traffic based on the dest addr of the packet and again a static arp entry for the ho