

Re: How to hard wire arp tables? (Newbie)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2001-11/0037.html>

From: Jose Nazario (jose@biocserver.BIOC.cwru.edu)

Date: 11/14/01

Date: Wed, 14 Nov 2001 14:02:26 -0500 (EST)
From: Jose Nazario <jose@biocserver.BIOC.cwru.edu>
To: "brad's @ Home" <nelson.brad@home.com>
Subject: Re: How to hard wire arp tables? (Newbie)
Message-ID: <Pine.LNX.4.30.0111141358230.11799-100000@biocserver.BIOC.CWRU.Edu>

On Wed, 14 Nov 2001, brad's @ Home wrote:

> *I want to hardwire my arp tables on a lan to protect against man in
> the middle attacks. I am using Redhat 7.1 and my install didn't
> include the file /etc/ethers. I created the file putting "mac
> address" (space) "ip address" as the man page directed. However, a
> book I have called for the opposite "ip address" (space) "mac
> address". I then add the line "apr -f /etc/ethers" to the end of my
> rc.local file. Next I ran the ./rc.local to reload the script.*

from my older arp manpage:

`-s hostname hw_addr`

Manually create an ARP address mapping entry for host hostname with hardware address set to hw_addr class, but for most classes one can assume that the usual presentation can be used. For the Ethernet class, this is 6 bytes in hexadecimal, separated by colons.

`-f filename`

Similar to the `-s` option, only this time the address info is taken from file filename set up. The name of the data file is very often /etc/ethers, but this is not official.

The format of the file is simple; it only contains ASCII text lines with a hostname, and a hardware address separated by whitespace.

you can use either `arp -s` or `arp -f /etc/ethers` to achieve the same effect: statically add entries, which is what you want to do.

what did you see when you reran `arp -a`? i get errors when i try and add static entries, but when i delete them before i `arp -s` them i get it ok:

SecurityFocus Linux: Re: How to hard wire arp tables? (Newbie)

? (192.168.208.1) at 00:30:85:2b:94:02

? (192.168.208.2) at 00:00:1d:1f:4f:12 static

the "static" keyword at the end is what you want to see. i had to arp -d 192.168.208.2 and then readd it with arp -s to get that to work. flush your arp table (arp -d -a) then readd the ones you want statically (arp -f or arp -s). that may be it.

jose nazario jose@cwru.edu

PGP: 89 B0 81 DA 5B FD 7E 00 99 C3 B2 CD 48 A0 07 80

PGP key ID 0xFD37F4E5 (pgp.mit.edu)

- **Previous message:** ksemat@wawa.eahd.or.ug: "[Re: Keeping remote root access to a compromised network – question](#)"
- **In reply to:** [brad's @ Home](#): "[How to hard wire arp tables? \(Newbie\)](#)"
- **Next in thread:** [Scott Gifford](#): "[Re: How to hard wire arp tables? \(Newbie\)](#)"
- **Next in thread:** [Vincent Danen](#): "[Re: disable 'su' for normal users](#)"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)