

RE: mac duplication

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2003-12/0024.html>

From: Demar, Jeremy D CTM1 (CCDG12 Aug) (*DemarJD_at_ccdg12.navy.mil*)

Date: 12/14/03

To: vuln-dev@securityfocus.com
Date: Sun, 14 Dec 2003 14:48:30 -0500

Another solution you could use depends on your switch. I've used several that allow you to do port mirroring. All you would have to do is tell the switch to mirror the port that the computer you want to monitor is on to the one your sniffer computer is on and turn on your sniffer. All traffic destined for your target will be copied to you. I used a similar setup for running snort and mirroring the port that my router was on.

Jeremy

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

From: Jimi Thompson [mailto:jimit@myrealbox.com]

Sent: Saturday, December 13, 2003 7:34 PM

To: vuln-dev@securityfocus.com

Subject: Re: mac duplication

Dev,

You seem to need some clarification about how Ethernet actually works. I'm going to try to toss out a 50,000 foot view. Anyone can feel free to add to this or correct me. Host names map to IP addresses via DNS. IP address map to MAC addresses via router tables. Just as your IP address has to be unique in order to be routable, so does your MAC address. MAC addresses are purchased in blocks by the people who make network devices and blown on to what amount to EPROMS and attached to network cards, switch ports, etc.

No two ethernet cards on the planet should have the same MAC address (emphasis on SHOULD because I've run into cards with duplicated MAC's and you won't believe the havoc this wreaks). This is used as a physical layer address by things like ARP.

If you want to sniff traffic to a particular machine, get yourself a hub (NOT a switch) and plug the switch into the uplink on the hub and your sniffer and sniff-ee into the hub ports.

This will A) let you see everything and B) not cause any serious problems for your switch. I hope that no one was using the machine you

RE: mac duplication

SecurityFocus Vuln-Dev: RE: mac duplication

were trying to sniff because chances are you are causing a DOS situation by duplicating the MAC address.

Jimi

Dev wrote:

>hi ppl, please redirect me to a different mailing list if this is not the appropriate list to post to.

>

>I did the following experiment:

>

>I have a switched ethernet network in my university.

>I wanted to capture packets meant for a certain machine on a different port of a Dlink switch. I thought that arp poisoning would be too noisy – arpwatc can catch it, & its too bulky for the MITM machine (in case we are poisoning a heavily loaded server machine.)

>& So i duplicated the mac of the victim machine on my own machine.

>

>What i saw was this:

>

>ping packet drop rate for any of the two machines from a third machine varied from 40 to almost 80 %. Also say telnet sessions to any of the two machines (which had now the same mac addresses) worked with notable 4–5 second lockups.

>

>Further i could not ping the other machine from one of the duplicated machines. (the last one is okay – it makes a lot of sense)

>

>My premise is that the problem in connectivity is coming becoz the OS does not fall back to half duplex mode when two machines take up the same mac address??

>

>can anyone plz tell me about the behaviour. How do i set up mac duplication in that case so that i can sniff data.

>

>I dont want to hurt network performance. & so dont want to do mac flooding. Anyways i m not even sure the switches we have here would resort to broadcast mode in case of mac flooding.

>

>Last but not the least its my second message to the list, & people were really helpful in discussing about my queries in my first message.

>

>Mailing lists rock..

>

>Devrat

>

>

>

>

RE: mac duplication