

## RE: Rogue IP Address

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-05/0060.html>

---

**From:** Jose Guevarra ([jose\\_at\\_iquest.ucsb.edu](mailto:jose_at_iquest.ucsb.edu))

**Date:** 05/04/03

To: <[security-basics@securityfocus.com](mailto:security-basics@securityfocus.com)>

Date: Sat, 3 May 2003 23:18:32 -0700

I think we can narrow down solutions by understanding what type of equipment is being used here. nobody seems to know anything about Asante switches.

Andy, could you give us some specs on it, capabilities and such. You said that the port to IP feature wasn't working? well that's a very high level capability that you paid for when buying the switch, it should work. Why isn't it working now?

I would also suggest doing a fast ping scan of you subnets and grabbing MAC addresses from you arp tables. then start narrowing down who they belong to. Are you using DHCP reservations?

hth

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

From: Alaric Darconville [<mailto:alaric@cowboy.net>]

Sent: Friday, May 02, 2003 12:08 PM

To: [security-basics@securityfocus.com](mailto:security-basics@securityfocus.com)

Subject: Re: Rogue IP Address

I have seen a few responses to this stating to block that IP address at the router, or to reassign that address to another machine, in the hopes that someone will holler about his network not working. But someone intentionally using an IP address different from what they were assigned is probably not going to turn himself in like that. It would be akin to driving a stolen police car to the city garage and having the engine looked at.

It might be as simple as someone mis-entering the IP when setting up the system, but if it's a Linux machine then it's probably not doing the same things the user's ordinary workstation would be doing, therefore, he'd have to leave that machine running. On the other hand, he may have a dual-boot configuration on his machine, in which case, the IP he's usually assigned won't always show up on the network (disappearing when he reboots to go to his Linux setup). Perhaps the IP he's using is some sort of accidental transposition of characters (171 instead of 117, for

## SecurityFocus BASICS: RE: Rogue IP Address

example.) But if no IP's dropped off the face of the earth when the new one started showing up, it's definitely "IP theft." He's not going to call tech support, he'll just switch to another stolen IP. For the most part, you're going to have to assume that he knows what he is doing is wrong. Forget trying to get him to call when that machine can't connect.

Looking for extra machines in the area may help track it down. Pinging it to get the MAC address from the Arp cache will identify the machine a bit further. Trying to telnet to standard ports (25, 110, 23, etc) may reveal banners to help identify it. Maybe you'll be lucky and the sendmail banner displays "220 masterofpuppets ESMTP Sendmail 8.11.5" etc.... Look for the huge Metallica fan in the building :)

Alaric Darconville

Andy (dondon@pacbell.net) wrote:

>Someone on our network assigned an IP address to their own system  
>without my knowledge. Using LANguard network scanner, the best I can  
>tell is that it's a Linux box. The port-to-IP mapping table on our  
>Asante switch doesn't seem to work correctly.  
>  
>Any suggestions on tracing down that system that is associated with the  
>IP is appreciated!

Andy

---

FastTrain has your solution for a great CISSP Boot Camp. The industry's most

recognized corporate security certification track, provides a comprehensive prospectus based upon the core principle concepts of security. This ALL INCLUSIVE curriculum utilizes lectures, case studies and true hands-on utilization

of pertinent security tools. For a limited time you can enter for a chance to win one of the latest technological innovations, the SEGWAY HT.

Log onto <http://www.securityfocus.com/FastTrain-security-basics>

---

---

FastTrain has your solution for a great CISSP Boot Camp. The industry's most

recognized corporate security certification track, provides a comprehensive prospectus based upon the core principle concepts of security. This ALL INCLUSIVE curriculum utilizes lectures, case studies and true hands-on utilization

of pertinent security tools. For a limited time you can enter for a chance to win one of the latest technological innovations, the SEGWAY HT.

Log onto <http://www.securityfocus.com/FastTrain-security-basics>

---