

## RE: rogue IP address

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-05/0012.html>

---

**From:** Burton M. Strauss III (*BStrauss\_at\_acm.org*)

**Date:** 05/02/03

To: <security-basics@securityfocus.com>

Date: Thu, 1 May 2003 17:39:54 -0500

Sometimes, the alert from the LAN management software can be enough – if it shows the MAC addresses involved. For example, if it's a D-Link MAC address – see the OUI list at the IEEE – and all you have are 3Com NICs, well, the hardware probably won't look like any of your other machines either and may stand out to a visual audit (that's IT speak for walking around being nosy poking you head into cubicles and offices looking for hardware you don't recognize).

Thoughts...

Program the switch to drop that IP address – see who screams. If the switch won't do it for you, you may have to get brutish here – build a transparent filtering bridge and drop the packets that way.

Try using tcpdump to see if you can sniff the packet streams and run something like strings on it. It may give you login names etc. that you recognize.

```
tcpdump -w x.raw -c50
strings x.raw | grep USER
strings x.raw | grep PASS (Since people use their mail address for
anonymous ftp)
```

etc.

(This one is a real PITA, but it works – I've done it successfully) On the weekend, unplug each of your backbone switch segments, one at a time and see when the rogue drops off the network. Then follow it down to (ultimately) a single LAN segment and thence to a specific physical port. Remove said box and ransom it back at the cost of an agreement to play nice in the future.

If you can't do those, here's a sneaky way that sometimes works – build your own Linux box and give it that address and MAC address. Put it on the network backbone, so everybody sees it as "real close". It should cause various routing tables and switches to prefer your box and thus disable the rogue. See who screams.

SecurityFocus BASICS: RE: rogue IP address

-----Burton

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

From: dondon@pacbell.net [mailto:dondon@pacbell.net]

Sent: Wednesday, April 30, 2003 5:40 PM

To: security-basics@securityfocus.com

Subject: rogue IP address

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 see 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>

---