

## Re: Identification of non Cisco AP's

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-07/0336.html>

---

**From:** Chuck (*chuck.lists\_at\_gmail.com*)

**Date:** 07/27/05

Date: Wed, 27 Jul 2005 10:04:18 -0400

To: security-management@securityfocus.com, pen-test@securityfocus.com

I would guess that most of these access points would have ports 80 and/or 443 open for management. So you could get down to a short list by scanning for those ports (assuming your network doesn't have a whole bunch of other web servers). You could do this with nmap, if that takes too long, with scanrand. Nmap can use a file full of networks to scan with the `-iL` switch, so you don't have to scan the whole Class A.

Then, when you have a list of systems with those ports open, you run a little banner grabber script to do a HEAD or GET on each server and you should be able to identify what they are from the Server: header. If this doesn't give enough info, just pull up the page in a browser.

If they don't have a web interface available to your side of the network (which would be the case if they are a home router/firewall/ap type of device) you could try OS fingerprinting the network with nmap or xprobe, but that will take a while and these devices probably won't respond so that may not be easy. You may be able to identify these devices by the fact that they don't respond, but you would have to know the IP is in use from DHCP logs or traffic analysis. If there are large enough broadcast domains or if you have IDSs deployed or are using DHCP, you may be able to identify these devices by MAC addresses, but again, most of these devices can spoof their MAC. In short, it may be easier to wardrive/walk around your area if the network is in one physical location.

Good luck.

Chuck

On 7/26/05, Jonathan Gauntt <jon0966@yahoo.com> wrote:

> Hi,

>

> *I have been tasked with the project of scanning and identifying all non*

> *Cisco wireless access points within the company's network.*

>

> *We have about 800 /22 and /24 subnets, and because of the IP addressing*

## SecurityFocus Penetration: Re: Identification of non Cisco AP's

- > *scheme in place, might just be easier for me to scan the whole class A range*
- > *of IP's.*
- >
- > *I have access to Nessus and GFI Security Scanner. Since we over 8000 IP's*
- > *in place, does anyone have any advice on the best way to identify these non*
- > *Cisco AP's such as Linksys and Netgear, etc.*