

RE: Detecting WAP's

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2002-01/0088.html>

From: Woody.Hughes@WellsFargo.COM

Date: 01/03/02

From: Woody.Hughes@WellsFargo.COM

To: list@mcclincy.com, security-basics@securityfocus.com

Date: Thu, 3 Jan 2002 13:43:37 -0800

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Actually, you could try to monitor for Request to Send packets and CTS packets.. Basically, 802.11b use carrier sense multiple access with collision avoidance. CSMA/CA if I remember correctly. That's how wireless networks deal with collisions. Basically, it's a four-way handshake communication, so what you have is RTS (Request to Send) with the address set to the intended destination. Then, if the destination address receives it, it'll send a CTS (Clear to Send) packet back. Then the original machine that started the handshake will begin sending the payload, and after it's all finished, the receiver will send an ACK back...

Now...you could, theoretically, monitor the RTS and CTS packets. But, I haven't done it. But that would be the one thing to watch out for. Then again, in order to monitor these packets, you're going to have to monitor air traffic with something like AirSnort or something like that...

But you can also startup with the notion that, if someone has added an AP to the network, and they've enabled WEP with a 128-bit key, you're now going to have to run a sniffer for 24 hours, depending on the traffic going through it, in order to break the key, and be able to start sniffing the actual data. Then again, I'm probably getting a little too far into this considering that you just want to detect whether or not you have an AP on the network.

I'm sure there's others on the list that have done this, and have more experience than I, so maybe they can lend a thought to this discussion...

/*

* Woody Hughes

* Sr. Info Security Analyst

RE: Detecting WAP's

SecurityFocus BASICS: RE: Detecting WAP's

* Security Products Services
* Corporate Information Protection Division
* -----
* woody.hughes@wellsfargo.com
* Phone: 415.243.5846
* Fax: 415.975.7468
*/

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

From: sim [mailto:list@mcclincy.com]
Sent: Wednesday, January 02, 2002 2:58 PM
To: security-basics@securityfocus.com
Subject: Detecting WAP's

Hello,
I spent the better part of my morning today tracking down a WAP within my building. We basically stumbled onto the signal by blind luck (testing a WAP enabled laptop) and I proceeded to walk around on a few floors searching cubicles until I found it sitting inside someone's cabinet.

My current network policy is no wireless devices.

My question is how does one proactively monitor for a WAP in a standard routed/switched environment. Is there any intelligent way to accomplish this? I would be interested in ideas/solutions for LAN's and WAN's. Is there something I can look for within each packet or perhaps specific types of traffic (broadcast?) create by the WAP?

Unfortunately I am not up on 802.11 (yet) and this recent incident has me concerned given anyone within range had free access to my network.

Any comments, links, documents, or criticisms are welcome. Please respond to the group.
CM

-----BEGIN PGP SIGNATURE-----

Version: PGP 7.0.4

iQA/AwUBPDTQhXuWMfODQZohEQLgxQCeILtTci//DVxmWEc1p7C+oUtgoZwAoM5J
AFgKWxhbzLfrdLeDF/avl+jg
=FO6Y

-----END PGP SIGNATURE-----

SecurityFocus BASICS: RE: Detecting WAP's

- *Previous message:* Douglas Pichardo: "Re: Is there any free replacement for zone alarm ?"
- *Maybe in reply to:* sim: "Detecting WAP's"
- *Next in thread:* John Morris: "Re: Detecting WAP's"
- *Messages sorted by:* [date] [thread] [subject] [author] [attachment]