

RE: IDS & Wireless Access Point Detection

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2002-03/0014.html>

From: Moser Max (MMoser@3gmobile.ch)

Date: 03/04/02

Date: Mon, 4 Mar 2002 09:45:01 +0100
From: "Moser Max" <MMoser@3gmobile.ch>
To: <FOCUS-IDS@securityfocus.com>

Hi all,

At <http://www.remote-exploit.org> you will find wellenreiter. Wellenreiter is a small perl based project that tries to

Combine wireless penetration techniques together into one perlgtk tool. I develop this tool with the team from remote-exploit.org. The current release only do statistics etc. But in the next few days I release the new version with the

Analyzer window built in. This windows does detect accesspoints (Broadcasting or not), cards communicating with other

Cards, detection of ad-hoc networks. The detection of the network (WEP) parameters are in progress. It supports channelswitching and at the moment the analyzer runs on the cisco based cards only. But it depends only on the way

To get the packet. Btw it does all the things using raw-mode.

I did also a small modification of my first 802.11b decoder to alarm when a "stolen card" tries to do somethin in

The air. So I can find those people that told us that they have lost your cards :-).

I still search for some people that got knowledge in perl and 802.11b for developing. Betatesters are also welcome,

Because unfortunaly I don't got much response but a hughe amount of downloads.

Greetings

Max Moser

<http://www.remote-exploit.org>

> -----Original Message-----

> From: mstokes@cdhelp.com [<mailto:mstokes@cdhelp.com>]

> Sent: Friday, March 01, 2002 4:52 PM

> To: FOCUS-IDS@securityfocus.com

> Cc: jshenk@decommunications.com

> Subject: RE: IDS & Wireless Access Point Detection

>

>

> Netstubler or minix will not account for all AP's. Any AP not in

SecurityFocus IDS: RE: IDS & Wireless Access Point Detection

> broadcast mode or programmed not to respond to probe requests will
> not be detected. If you have a wireless network then invest in
> AiropEEK from Wildpacket will detect all 802.11b (for now) at the LLC
> layer and up.

>
> Barring the purchase of AiropEEK trapping for known MAC's of wireless
> devices is a good idea however, remember it is easy to spoof your MAC.
> This said it should catch most Saturday warriors.

>
> If you're very concerned vis-à-vis wireless then do a RF footprint of
> business. Change antenna location, use yagi's for point to point, and
> at a minimum turn WEP on (it might be broken but at least it's a
> deterrent and it demonstrates that your LAN is a closed system.) Just
> some ideas from RF hell out here in California

>
> Michael Stokes
> CD\Help, LLC
> Security/Forensics & LAN/WAN/WLAN Engineering Firm

>
>
> -----Original Message-----
> From: Jerry A. Shenk [mailto:jshenk@decommunications.com]
> Sent: Friday, March 01, 2002 10:23 AM
> To: FOCUS-IDS@securityfocus.com
> Subject: RE: IDS & Wireless Access Point Detection

>
>
> I'm not sure how a PCI card in infrastructure mode would do....I think
> that would open you up to people attaching to that from the outside.

>
> How about just using netstumbler or ministumbler (running on an ipaq
> or some other ce) and walk around the building periodically. I think
> this is probably the best idea. You could have that ipaq running with
> ministumbler in your pocket all the time and if you ever got in range
> of an AP, it could 'go off' and you could follow the signal strength
> to track it down.

>
> Another thing I've used is collecting ARP tables from routers and
> searching through that for MAC addresses of known APs. I only did
> that once as a 'quick n dirty' check for a customer.

>
> > -----Original Message-----
> > From: Rob.Hanson@stpaul.com [mailto:Rob.Hanson@stpaul.com]
> > Sent: Friday, March 01, 2002 11:29 AM
> > To: FOCUS-IDS@securityfocus.com
> > Subject: IDS & Wireless Access Point Detection

> >
> >
> > Hello:
> >
> > I currently manage a global deployment of NIDS sensors and am

SecurityFocus IDS: RE: IDS & Wireless Access Point Detection

> > *interested in detecting rogue access points that are brought up.*
> > *Our current security policy does not allow for 802.11x*
> > *communications and we're looking for a way to enforce this from a*
> > *corporate level. The NIDS run on Linux and I am considering*
> > *installing a cheap wireless PCI card, with prismdump and integrating*
> > *the logs generated by detecting a new AP into the*
> *IDS console.*
> >
> > *Is anyone else doing this with their IDS deployment? Are there any*
> > *gotcha's I should be considering (outside of detecting other*
> > *companies APs on the same block). If I put my NIC in Infrastructure*
> > *Mode, am I safe from someone hacking the IDS looking for a peer to*
> > *peer NIC, or are there other hardening considerations for this?*
> >
> > *Thanks in advance for any ideas you wish to share.*
> >
> > *-Rob.*
> >
> >
>
>

- **Previous message:** [Bill Royds: "Paper by Vern Paxon on normalizing traffic before it reaches NIDS"](#)
- **Maybe in reply to:** [Rob.Hanson@stpaul.com: "IDS & Wireless Access Point Detection"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)