

Re: Rogue AP Wireless on Windows/Linux

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-04/0036.html>

From: Franck Veysset (franck.veysset_at_rd.francetelecom.com)

Date: 04/11/05

Date: Mon, 11 Apr 2005 08:12:45 +0200

To: "szynkro@gmail.com" <szynkro@gmail.com>, pen-test@securityfocus.com

Honeygot...

You should have a look at Wireless honeypot. For a good start:

<http://www.honeyd.org/configuration.php>

You can also find some interesting information on securityfocus web site:

<http://www.securityfocus.com/infocus/1761>

Using honeyd on Linux, you can do almost whatever you want to simulate a Wireless AP, and trick Wifi client.

Cheers,
-Franck

szynkro@gmail.com said the following on 08/04/2005 19:52:

> *Hi,*
>
> *I'm looking for a way/all in one tool to simulate a wireless Access*
> *Point on a Windows XP and/or Linux system preferably with built-in*
> *DHCP daemon and all.*
> *The goal is to see if we can trick wireless clients in connecting to*
> *the AP, sniffing for potential credentials and other interesting stuff*
> *etc...*
>
> *I've heard about hotspotter, airsnarf and alike but don't know if*
> *they are valid...*
>
> *The scenario would be sniffing the unknown wireless network for valid*
> *SSID's and setting the SSID on the rogue AP.... then fingers crossed I*
> *guess that signal is strong enough to get some clients connecting. Can*
> *we force/help the client in associating with the rogue AP?*
>
> *Anyone some other valid (recent) Wireless Pen-Test scenario's?*
>
> *thanks*
>

--

Re: Rogue AP Wireless on Windows/Linux

SecurityFocus Penetration: Re: Rogue AP Wireless on Windows/Linux

Franck VEYSSET - & france telecom - R&D Division/MAPS/NSS
Research Engineer - Internet/Intranet Security