

SecurityFocus Penetration: RE: MORE: Tools for Detecting Wireless APs – from the wire side.

RE: MORE: Tools for Detecting Wireless APs – from the wire side.

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-06/0044.html>

From: Isherwood Jeff C Contr AFRL/IFOSS (Jeffrey.Isherwood@rl.af.mil)

Date: 06/10/02

From: Isherwood Jeff C Contr AFRL/IFOSS <Jeffrey.Isherwood@rl.af.mil>

To: 'Pierre Vandevenne' <pierre@datarescue.com>

Date: Mon, 10 Jun 2002 17:54:37 -0000

I mis-typed myself.

I called Netstumbler a "wrong answer" not because it is bad, or doesn't do the job, just NOT the job I'm looking for.

Mainly, I'm trying to figure out a companion for wardriving with a Stumbler. Anyone who relies on only one method of scanning, is leaving themselves open to potential gaps in the scanner's ability to cover.

A NETWORK – WIRED scan, detect method to compliment the wardriving Stumbler is helpful as a corroborative tool to help get a "second opinion" of sorts...

The two prevailing methods seem to be using the ARP cached MAC addresses to ID potential APs, and NMAP'd fingerprints of nodes compared to a list of AP Fingerprints...

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

From: Pierre Vandevenne [<mailto:pierre@datarescue.com>]

Sent: Monday, June 10, 2002 1:42 PM

To: Isherwood Jeff C Contr AFRL/IFOSS

Cc: 'Pen-Test'

Subject: Re: MORE: Tools for Detecting Wireless APs – from the wire side.

Hello Isherwood,

IJCCAI> MOST received wrong answer ??

IJCCAI> Netstumbler: Wardrive your own campus before they do.

IJCCAI> This is not always a practical, or failsafe method. You

IJCCAI> might miss an area, or your campus might be too big to

IJCCAI> realistically do this (imagine a corporation or Edu that is

IJCCAI> spread out over a mile or more, and your manpower is limited?)

RE: MORE: Tools for Detecting Wireless APs – from the wire side.

SecurityFocus Penetration: RE: MORE: Tools for Detecting Wireless APs – from the wire side.

I don't think it is a "wrong" method. As a matter of fact, each time I have tried it in a favourable environment, it has found many more APs than other methods combined. If there is one thing that you can't hide it is the radio traffic. It's true that SNMP can, in some cases, be disabled. But MAC addresses can be changed as well.

Large campuses are the easiest to scan. Get a high gain antenna and a golf cart and explore the area boustrophedonically.

The most difficult places to scan are actually medium sized organizations in a "downton-like" environment, where you pick up a lot of stuff that doesn't belong to you or where APs will remain hidden because of the faraday cages properties of some areas.

Interestingly, leaving aside the issue of regulations and power of emission, it is often much easier to stumble in the US than in Europe because of the wooden structure of many US buildings.

--

Best regards,
Pierre

mailto:pierre@datarescue.com

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- **Previous message:** [Kohlenberg, Toby: "RE: Tools for Detecting Wireless APs – from the wire side."](#)
- **Maybe in reply to:** [Isherwood Jeff C Contr AFRL/IFOSS: "MORE: Tools for Detecting Wireless APs – from the wire side."](#)
- **Next in thread:** [R. DuFresne: "RE: MORE: Tools for Detecting Wireless APs – from the wire side."](#)
- **Next in thread:** [Larry Youngquist: "Re: Tools for Detecting Wireless APs – from the wire side."](#)
- **Reply:** [R. DuFresne: "RE: MORE: Tools for Detecting Wireless APs – from the wire side."](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)