

RE: Mapping wireless LANS from the wired side

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-08/0117.html>

From: Mike.Ruscher@CSE-CST.GC.CA

Date: 08/23/01

Message-ID: <A7896A2B763AD511B27C00AA0DD93711FF21F@niagara.its.cse.dnd.ca>

From: Mike.Ruscher@CSE-CST.GC.CA

To: dcdave@att.net

Subject: RE: Mapping wireless LANS from the wired side

Date: Thu, 23 Aug 2001 13:58:17 -0400

Thanks. wap-nmap is "The mobile equivalent to the award winning nmap. What wap-nmap allows you to do is port scan a machine for open connections from anywhere. All via your WAP enabled phone. Highly useful for system administrators and network security specialists who are constantly on the go."

It can be downloaded without registration from <http://www.hackinthebox.org/article.php?sid=1200>.

This would still only scan from the wireless side, but is still an interesting tool.

mgr

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

From: dcdave [mailto:dcdave@att.net]

Sent: Tuesday, August 21, 2001 12:25 PM

To: Mike.Ruscher@CSE-CST.GC.CA; jshaw@insync.net

Cc: pen-test@securityfocus.com; woody@callisma.com

Subject: Re: Mapping wireless LANS from the wired side

There is a wap-nmap available – not sure this is what you are looking for, but

check fyodor's site, or I have a link to it at

<http://securingwireless.intranets.com>

(free resource page)

dcdave

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

From: <Mike.Ruscher@CSE-CST.GC.CA>

To: <jshaw@insync.net>

Cc: <pen-test@securityfocus.com>; <woody@callisma.com>

Sent: Monday, August 20, 2001 5:25 PM

Subject: RE: Mapping wireless LANS from the wired side

SecurityFocus Penetration: RE: Mapping wireless LANS from the w

- > *I have no doubt that the wired side is the best approach for mapping one's*
- > *own KNOWN wireless clients and APs. However, the question I originally*
- > *posed*
- > *concerns testing for active wireless devices on a network from the wired*
- > *side using wired LAN systems.*
- >
- > *There is no guarantee that war-driving will find them all, especially when*
- > *they may roam and not always be up when sniffed by a wireless system. In*
- > *any*
- > *case, this is irrelevant to the requirement at hand.*
- >
- > *What I am looking for I guess, is a "wmap" type of solution. (Fyodor?!)*
- >
- > *It's like finding dial-up modems from the network side, not by*
- > *war-dialling*
- > *(or by war-driving in this instance). In this case it should be a lot*
- > *easier, since everything is TCP/IP still. A list of company device/MAC*
- > *associations is all that would be necessary is my guess and not just*
- > *company/MAC associations. Collecting them is not a great hardship I*
- > *suppose*
- > *though, by time-consuming and forever requiring support to be fresh and*
- > *complete.*

>
> mgr

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

- > *From: Joe Shaw [mailto:jshaw@insync.net]*
- > *Sent: Monday, August 20, 2001 6:06 PM*
- > *To: Mike.Ruscher@CSE-CST.GC.CA*
- > *Cc: pen-test@securityfocus.com; woody@callisma.com*
- > *Subject: RE: Mapping wireless LANS from the wired side*

>
>
>
> *On Mon, 20 Aug 2001 Mike.Ruscher@CSE-CST.GC.CA wrote:*

- >
- >> *Yes, MAC addresses by vendor will identify the device company, if one*
- >> *can*
- >> *assume they are valid and not spoofed. I do not see on the OUI site*
- >> *where*
- >> *the MAC addresses are associated with a company's particular device*
- >> *family*
- >> *though. This is essential for determining a wireless device from a wired*
- >> *one. Do most companies give this info out, or must it be extrapolated*
- >> *from*
- >> *experience?*
- >
- > *The best way to track down wireless gear is with your own wireless gear.*
- > *It's much easier than trying to find them using the wired LAN. Trying to*
- > *find it any other way will just waste your time.*

SecurityFocus Penetration: RE: Mapping wireless LANS from the w

> *Regards,*
> --
> *Joseph W. Shaw II*
> *Network Security Specialist/CCNA*
> *Unemployed. Will hack for food. God Bless.*
> *Apparently I'm overqualified but undereducated to be employed.*
>
>

--
> 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/>
>
>

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:** [Dave Aitel: "New tool for you: dctest"](#)
- **Maybe in reply to:** [Mike.Ruscher@CSE-CST.GC.CA: "Mapping wireless LANS from the wired side"](#)
- **Next in thread:** [Mike.Ruscher@CSE-CST.GC.CA: "FW: Mapping wireless LANS from the wired side"](#)
- **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)