

Re: Mapping wireless LANS from the wired side

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-08/0102.html>

From: anindya (anindya@goonda.org)

Date: 08/20/01

Date: Mon, 20 Aug 2001 11:59:38 -0400 (EDT)
From: anindya <anindya@goonda.org>
To: <Mike.Ruscher@CSE-CST.GC.CA>
Subject: Re: Mapping wireless LANS from the wired side
Message-ID: <20010820113829.C93525-100000@phat.bastard.net>

It seems most of the wireless APs I have encountered all do things differently. For example, SMC 2652W AP will respond to a UDP packet to address 255.255.255.255 port 800 --- like so (.3 is the scanning host, .128 is the SMC AP):

```
11:46:20.928530 192.168.1.3.800 > 255.255.255.255.800: udp 60
11:46:20.945761 192.168.1.128.800 > 255.255.255.255.800: udp 59
```

A lot of the Prism2-based APs seem to use this method.

The lucent RG-1000, on the other hand, sends a UDP packet to port 192 of the network broadcast address (.4 the scanning host and .164 being the AP):

```
11:52:46.488720 192.168.1.4.2159 > 192.168.1.255.192: udp 116 (DF)
11:52:46.489443 192.168.1.164.192 > 192.168.1.4.2159: udp 116 (DF)
```

You can use the CLIproxy software provided by Lucent to find Lucent APs on the local subnet: i.e. "show accesspoints". An additional note about the RG-1000 is that they are configurable through SNMP, and nmap will correctly fingerprint them (-O).

You can always craft these packets (instead of using vendor's software) and see if any device responds after you inject them into the network.

Some other default SSIDs/login accounts can be found here:

http://www.wi2600.org/mediawhore/nf0/wireless/ssid_defaults/ssid_defaults-1.0.5.txt

thanks,
--Anindya

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

Re: Mapping wireless LANS from the wired side

SecurityFocus Penetration: Re: Mapping wireless LANS from the w

- > *This issue may have been discussed earlier but my search failed to find*
- > *anything definitive.*
- >
- > *When mapping a LAN topology, what are the general methods to use for*
- > *discovering access points and wireless hosts from inside the wired network.*
- > *This becomes important to detect rogue WLANS which are a potential threat to*
- > *the enterprise as they might be behind firewalls etc.*
- >
- > *I would expect that the MAC addresses for APs would be unique to the various*
- > *vendors., as would the wireless NICs on the WLAN hosts. Are there any*
- > *scanning tools freely available that can do this kind of search?*
- >
- > *Mike Ruscher, ITS Specialist I2, CSE/CST*
- > *mgruscher@cse-cst.gc.ca*
- > *Phone: +1 613 991-8040*
- > *ED/C200*
- > *<http://www.cse-cst.gc.ca>*
- >
- >

-
- > *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:*** [woody weaver: "RE: Mapping wireless LANS from the wired side"](#)
- ***In reply to:*** [Mike.Ruscher@CSE-CST.GC.CA: "Mapping wireless LANS from the wired side"](#)
- ***Next in thread:*** [Ichinin: "Re: Mapping wireless LANS from the wired side"](#)
- ***Reply:*** [Ichinin: "Re: Mapping wireless LANS from the wired side"](#)
- ***Messages sorted by:*** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)