

Wardriving: Who's Browsing your Wireless Network

www.thesolutionfirm.com

Wardriving: Who's browsing your wireless network

Michael Gregg

Sales of wireless networking equipment are on the rise. More organizations are adopting it each day. Even though the overall awareness of security has never been higher, individuals seem to have no problems setting up unsecured wireless networks. Finding these unsecured networks has become quite a fad; hackers are making a game of driving around and connecting to as many networks as they can. Operating an unsecured wireless network is much like leaving your keys in a car, parked in a high crime neighborhood. You had better hope you're lucky!

What's the problem?

Many end-users who are moving to wireless don't have any appreciation of the security measures they should employ. Wireless Access Points (WAPs) require nothing more than power and a connection to an active RJ-45 jack. The default configuration has Wired Equivalent Privacy (WEP) security turned off. WEP was originally designed to protect wireless networks from eavesdropping through the use of a 40-bit key. The key was limited to 40 bits due to export rules that existed during the late 1990s when the 802.11 protocol was developed. This provides a very limited level of encryption that is relatively easy to compromise.

The technology also offers the option of a Service Set Identifier (SSID). The identifier is attached to packets sent over the wireless LAN and functions as a password within an ad hoc network. All devices within this network must share the same SSID. Most individuals never bother to change this from its default value, thereby decreasing security.

Defense requires offensive

There are ways to enhance your existing security. It may be a little work, but it's worth it! Remote home users should turn on WEP and change the SSID. This will provide a minimal level of protection. If the user is not using wireless on a full-time basis, unplug the WAP or place it on a timer so that it's off during those hours when no one's using the network. These safeguards won't keep a determined hacker out, but they will help keep honest people honest.

In a business environment, changing the SSID and enabling WEP is only the first step. Carefully consider the placement of your WAPs. Isolate these devices from critical portions of your network. Restrict the allocation of DHCP addresses on the wireless network segment. Prohibit access from unknown MAC addresses. Management must understand that to protect the confidentiality of network traffic, additional security measures such as IPsec will be required. An audit of your wireless network will demonstrate just how insecure it is.

Tools of the trade

Are you ready to check out your network? Make sure that management is aware of your actions. The last thing you want to do is explain why you're running cracking software on the company laptop. You'll need a wireless NIC, a good antenna, and some of the software listed below. You might want to consider building the infamous Pringles antenna.

Start by walking around your facility to see just how far your network extends. It's important to use the same tools that can be used against you. You will want to have a good idea of what unwanted guests can find out and how quickly they can enumerate your network. Use these tools to convince management that WEP really is insecure and to justify the needed changes.

WEPcrack: This software tool is for breaking 802.11 WEP secret keys. It operates by capturing and analyzing data as it moves across a wireless network. Don't be too surprised at how quickly it works!

Airsnort: This tool uses a completely passive attack. When enough information has been captured, the program will piece together the system's master password.

NetStumbler: This Windows-based network auditing tool can be used by administrators wanting to check the coverage of their wireless LAN and to verify that their corporate LAN isn't wide open.

ApSniff: Here is another WAP sniffer. It can help you document all access points broadcasting beacon signals at your location.

Ethereal: This industrial strength protocol analyzer can be used to capture and decode network traffic.

Don't be an easy target

Wireless is a great tool and can enhance productivity. Its architecture, however, is in a state of development. Look for improvements to the WEP protocol next year. Wireless Protected Access (WPA) is due for release during the first quarter of 2003. Presently, wireless networks need stronger protection and should be used in conjunction with other security technologies. Education and consumer awareness are the keys to developing this technology to its full potential. The only way to gain total network security is to unplug from the rest of the world, and that's not feasible in most situations. However, a little work can vastly decrease network vulnerability. Predators look for the easy targets. Make sure you are not one of them!

About the Author

Michael C. Gregg is the COO of Superior Solutions, Inc., a security assessment and training firm. His current responsibilities include performing security assessments and evaluations for corporate and government entities. He has served as the developer of high-level security classes, study guides, has taught classes for many Fortune 500 companies and contributed to many books, including the Sybex publication, *Security Administrator: Street Smarts*.

