April, 2005

Assessing the security of a wireless environment

By Michael Gough, John Rhoton

With the explosion of wireless networks and their adoption by companies of all sizes, the need to assess the security worthiness of the wireless environment should be considered a requirement not an option. It is our belief that if you deploy wireless you are obligated to manage the security on an ongoing and regular basis. This does not mean doing an occasional assessment, it means implementing an automated solution that monitors and alerts when anomalies are discovered.

Wireless can be deployed securely, but due to the nature of wireless and the ease in which it can be easily expanded by the addition of rogue access points (AP) by either a uneducated user, administrator or mis-configuration of an AP, openings can be introduced fairly easily so managing the wireless security becomes a full time responsibility.

There are numerous tools available for free and commercial tools that allow you to assess a wireless network (see ***Appendix A***), but how to use these tools and what to look for and how to interpret the information from these tools is a challenge for many of us who use them.

We must first start by defining the two types of assessment methodologies that are available and used to assess a wireless network.

1. Manual or Ad-Hoc Assessment
2. Automated Assessment

These two assessment techniques have far different approaches and results. A manual or Ad-hoc assessment is an assessment in a moment of time. An automated assessment is an ongoing assessment that monitors the wireless environment for any changes, additions or suspicious activity and alerts when detected.

Both of these methods have their place, but with the risks associated with having an insecure wireless network in your environment requires that both methods of assessment be used to assure a securely deployed wireless environment is deployed securely and stays securely deployed.

Manual Assessment

A manual assessment uses the typical tools we all know and read about in the rags that are used by young teens to adults looking for an open Access Point (AP) to surf for free. They include popular tools like NetStumbler, MiniStmbler, WiFiFoFum, AirSnort, and commercial tools like AirMagnet to name a few.

Manual assessments have their place as they are used to check the current operating condition of a wireless environment and also to verify that an automated assessment methodology is working. These assessments are tactical in nature as they are performed infrequently and are only good for the moment they are used. A rogue AP could be installed the next day and no one would know until the next manual assessment.

It is not recommended that an organization rely on an annual manual assessment to validate the security of a deployed wireless environment. It should only be used to verify the current state or that an automated assessment process is working as expected.

Automated Assessment

An automated assessment as the name implies is an assessment that is automated and working all the time monitoring the wireless environment for any changes or suspicious activity and alerts when a suspicious condition is detected.

With the risk that an insecure wireless device poses to any environment, it is recommended that the use and deployment of a wireless network that is intended to be secured have an automated assessment process to maintain the secured state. Networks like wireless hotspots that are by nature open and not used for anything other than internet access do not require an automated assessment process. These networks are open on purpose and users only need to be warned that any information they send over the wireless network is subject to being looked at unless a secure transport like a VPN is used.

The goal of an automated assessment methodology is that once you deploy a secure wireless solution, of which there are many, that your wireless network remains secure and if any suspicious anomalies show up, the automated assessment solution will alert the appropriate personnel that suspicious activity is occurring.

Pocket PC versus a Laptop

Before you decide what tools you might use, you might want to understand what tools work on what platforms so that you can make the best choice. 802.11b is built-in t many Pocket PC devices. Tools like MiniStumbler and WiFiFoFum that detect 802.11b wireless may also have the ability of seeing 802.11g networks as they behave very similar to 802.11b. What you cannot get on a Pocket PC is 802.11a as the spec does not have a 16bit client, so you will not be able to see 802.11a networks using a Pocket PC. So if you want to monitor for all types of 802.11, you will need to use a laptop running Windows XP or your favourite distribution of Linux.

So what do the free tools tell you?

The freeware or open source tools that exist were mostly designed to find open insecure networks. With that said you can use the free tools like NetStumbler, MiniStumbler and AirSnort to find wireless networks but the information they produce needs to be interpreted. First off if you see your wireless network in one of these tools, your network is most likely configured incorrectly or not as the Wireless Benchmark suggests, unless you want an open network in your environment. If you have a need for everyone to see your network for public access, seeing your network in these tools is NOT a desirable thing and indicates that your network is open for anyone to investigate and misuse.

Performing a Manual Assessment

The best tool for performing a manual assessment is a commercial tool. The free tools are nice to see what is most obvious, but a commercial tool is geared to reporting the results in detail versus just showing you an open Access Point. AirMagnet for example can perform 802.11a,b or g assessments on a Windows XP Laptop and print nice reports for your assessment results. In addition Airmagnet has a function to help you locate a potential open AP with a 'find' tool that sounds like a Geiger counter.

I use the free tools to see what the public would see. I then use AirMagnet to quickly make reports for my client or management.

AirSnort has the ability of cracking WEP keys, but I would never attempt this for a client. We all know by now that WEP is inadequate and not to use it unless you add another layer of security like a VPN for example. AirSnort shows substantially more than NetStumbler or MiniStumbler, but again only detection, no reporting.

We can also use NMap and a sniffer when we discover an unexpected open AP where there should not be one to see what is on the found wireless network, but usually finding the open AP is the reward, seeing the traffic is a foregone conclusion.

Other than being able to crack a WEP key, the free tools do not offer anywhere near what a commercial tool like AirMagnet does. Commercial tools provide what we need, detailed reporting.

If you want a recommendation for a manual wireless assessment tool, invest in a tool like AirMagnet or similar product and use the free tools as a secondary validation to what the commercial tool finds.

Automated Assessment

In an automated assessment methodology you have many options. Standalone solutions that have sensors you deploy to provide full coverage of your environment, IDS security functions that are built into the Access points or switches and authentication solutions that authenticate every wireless user. In addition you may even perform client health checks via a quarantine network to further reduce the threats from worms and viruses and/or to validate the user's adherence to client side security policy.

A recommendation as we suggested at the beginning of this document "the need to assess the security worthiness of the wireless environment should be considered a requirement not an option". If you already have a deployed wireless network in your environment or planning one, include an automated wireless assessment solution to protect yourself from accidental exposures or focused attacks through your wireless environment.

Intrusion Detection

There are many ways to approach rogue and decoy access points and other kinds of wireless intrusions:

Client-based software that runs on handhelds or laptops can allow you to physically roam your coverage area looking for unusual SSIDs, sources of interference and then pin-point their locations using a signal-strength indicator. Mention Net/Mini Stumbler WiFiFoFum Airmagnet, Snort (we are the users and they might want examples)

Access points can scan all channels regularly, checking for rogue or decoy access points and reporting them to an administrator.

Sensors can provide comprehensive coverage in time and space. Airmagnet AirDefense are a few.

Wireless switches can authenticate all access points ensuring that only authorized connections are allowed onto the corporate network. In many cases, the access points and sensor networks can signal suspicious traffic to the switches, which can use the information to block the irregular activity.

These techniques and the corresponding products vary in terms of being able to spatially position intrusions as well as their differentiation between intrusions and air-space overlap from neighbours. They also differ in their alert capabilities (Openview, e-mail, SMS). If you don't automate the detection of suspicious activity and alert… you should not deploy wireless…

A detailed product comparison of Wireless IDS vendors is beyond the scope of this document, but a few are worth a brief mention. AirMagnet and AirDefense are market leaders that have specialised in intrusion detection. Access points from Airespace and Trapeze Networks include periodic channel-scans. Cisco has also integrated limited rogue detection into its access points and can be enhanced with its Wireless LAN Solution Engine. Similarly, Aruba allows its access points to be configured as active access points or as sensors that sweep the spectrum.

From a pragmatic perspective, the enterprise requirement is not so much to identify a particular product that solves all threats of intrusion. Instead, it is necessary to ensure that comprehensive procedures, and supporting tools, are in place to actively monitor for wireless irregularities, provide an effective notification mechanism and then quickly isolate and remove the threat.

Quarantine

Air security and intrusion detection are effective measures to protect against malicious users gaining unauthorized access to the network. However, increasingly, another threat is becoming more prevalent. Naïve users, who do not adhere to the corporate guidelines for updating their systems, expose vulnerabilities in the infrastructure that can lead to disastrous consequences in the face of viruses, Trojans and worms.

In order to minimize these threats it becomes mandatory for the network to scrutinize connecting systems and verify that they are compliant before granting them full access to confidential resources. These system health checks also help to reduce the proliferation of malware between peers on the network and therefore conserve bandwidth.

There are two basic approaches to network quarantining which can be used in combination or separately:

Client-based – Software executes on the client and ensures that the platform is up-to-date with the corporate health policies – all patches have been applied; the latest anti-virus and intrusion-detection software is running with current signatures. The client must establish a cryptologically secure connection with the Network Access Server (NAS) (i.e. it should not be possible for a virus to replace the quarantine client) and report the state-of-health. Microsoft's Network Access Protection (NAP) is an example of this approach.

Network-based – The Network Access Server runs a series of probes against the connecting client looking for known vulnerabilities. For example, these might include scanning for open ports. Perfigo (now acquired by Cisco) CleanMachines offers network-based verification.

Of the two methods, there is no question that the client-based technique can provide a much more thorough check of the system's health. However, this must be balanced against the need for multi-platform clients the additional effort of remote installation.

Based on the results of the health check, the Network Access Server can either grant full access to the network or can fully reject the client request. However, the typical response to clients who do not fully comply with the corporate policies is not to categorically stop their network access. Instead, the NAS will impose stringent packet filters that isolate the client to a subnet where they can receive remedial support. This will include servers that host the latest software, signatures and patches as well as instructions for how to install them.

Summary

With the proliferation of rogue access points, it is in the best interests of every enterprise to ensure that it has a comprehensive WLAN security strategy. This begins with the detection of rogue and decoy access points, and other kinds of wireless intrusions. It must then provide a secure and robust mechanism for legitimate WLAN usage on the network, which equates to user-based authentication and encrypted air traffic.

Conclusion

Whatever solution you decide to deploy to assess or manage your wireless security, they all have the same goal – to monitor the wireless security and alert to anything suspicious. The CIS Benchmark helps you to decide how to deploy a wireless network securely and this article helps you to understand how to keep that wireless network secure.

References

Appendix A. Additional Resources

Wireless Sniffers

Netstumbler

www.netstumbler.com

http://www.netstumbler.com/downloads/

NetStumbler is a tool for Windows that allows you to detect Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g.

It has many uses:

- Verify that your network is set up the way you intended.
- Find locations with poor coverage in your WLAN.
- Detect other networks that may be causing interference on your network.
- Detect unauthorized "rogue" access points in your workplace.
- Help aim directional antennas for long-haul WLAN links.
- Use it recreationally for War Driving.

Kismet

http://www.kismetwireless.net/

Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic.

Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and infering the presence of non-beaconing networks via data traffic.

AirSnort

http://airsnort.shmoo.com/

AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

AirSnort, along with WEPCrack, which was released about the same time as AirSnort, are the first publicly available implementations of this attack.

AirSnort requires approximately 5-10 million encrypted packets to be gathered. Once enough packets have been gathered, AirSnort can guess the encryption password in under a second.

Airtraf

http://sourceforge.net/projects/airtraf

http://airtraf.sourceforge.net/

AirTraf is one of the first wireless 802.11(b) network analyzers. With the growth of interest in wireless networks, network administrators of today are faced with a challenge. The challenge is to effectively deploy numerous access points within their organization to provide wireless coverage for all users, and at the same time make sure that everyone who is granted access is able to operate in a fast, robust network environment.

AirTraf is a 100% passive packet-sniffing tool for the wireless 802.11b networks. It captures and tracks all wireless activity in the coverage area, decodes packets, and maintains acquired information associated by access points, as well as detected individual wireless nodes. It dynamically detects any access points in the area, finds association between wireless clients and access points, and builds information table for each packet that is transmitted via the air. AirTraf is able to maintain packet count, byte information, related bandwidth, as well as signal strength of nodes.

APhunter

http://www.math.ucla.edu/~jimc/mathnet_d/download.html

Access Point Hunter. It can find and automatically connect to whatever wireless network is within range. It can be used for site surveys, writing the results in a file.

AP Radar

http://apradar.sourceforge.net/

AP Radar is a Linux/GTK+ based graphical Netstumbler and wireless profile manager. This project makes use of the version 14 wireless extensions in linux 2.4.20 and 2.6 to provide access point scanning capabilities for most models of wireless cards. It is meant to replace the manual process of running iwconfig and dhclient. It makes reconfiguring for different APs quick and easy.

BSD-Airtools

http://www.dachb0den.com/projects/bsd-airtools.html

BSD-Airtools is a package that provides a complete toolset for wireless 802.11b auditing. Namely, it currently contains a bsd-based wep cracking application, called dweputils (as well as kernel patches for NetBSD, OpenBSD, and FreeBSD). It also contains a curses based ap detection application similar to netstumbler (dstumbler)

that can be used to detect wireless access points and connected nodes, view signal to noise graphs, and interactively scroll through scanned ap's and view statistics for each. It also includes a couple other tools to provide a complete toolset for making use of all 14 of the prism2 debug modes as well as do basic analysis of the hardware-based link-layer protocols provided by prism2's monitor debug mode.

Dstumbler

http://www.dachb0den.com/projects/dstumbler.html

Dstumbler is a wardriving/netstumbling/lanjacking utility for bsd operating systems that attempts to provide features similar to netstumbler in a fast and easy to use application. Dstumler is part of the bsd-airtools package released by Dachb0den Labs, which provides a complete bsd based tool set for 802.11b penetration testing.

Gtk-scanner

http://sourceforge.net/projects/wavelan-tools

802.11 network tools - allow for detection of networks and services initially using wireless extensions for linux (openbsd porting simple?) and raw 802.11 frames.

PocketWarrior PocketPC

http://sourceforge.net/projects/pocketwarrior/

PocketPC WiFi 802.11b Prism wardriving tool

Mognet, an 802.11b Protocol Analyzer in Java

http://node99.org/projects/mognet/

Mognet is a simple, lightweight 802.11b sniffer written in Java and available under the GPL. It features real time capture output, support for all 802.11b generic and frame-specific headers, text mode capture for GUI-less devices, and loading/saving capture sessions in libpcap format.

Mognet requires a Java Development Kit 1.3 or higher, and a working C compiler for native code compilation. Your wireless card must support monitor mode, which most (but not all) do.

802.11 based Linux software

http://www.guerrilla.net/gnet_linux_software.html

Some tools and drivers that are for Linux using prism based cards.

- cqureAP: Floppy Based Access Point
- NoCatAuth: Wireless Gateway Manager Package
- GNET AP Setup

- Wireless Tools Packages
- Prism I/ Prism II Linux Drivers

Prism Stumbler

http://prismstumbler.sourceforge.net/

Prismstumbler is a wireless LAN (WLAN) discovery tool which scans for beaconframes from accesspoints. Prismstumbler operates by constantly switching channels and monitors any frames recived on the currently selected channel.

Prismstumbler is designed to be a flexible tool to find as much information about wireless LAN installations as possible. It comes with an easy to use GTK2 front-end and is small enough to fit on a small portable system. Because of its client-sever architecture the scanner engine may be used for different front-end.

Pocket warrior

http://www.pocketwarrior.org/

This is wireless auditing software for PRISM and NDIS 5.1 compatible card that runs on PocketPC 2002. Pocketwarrior is now released under GPL.

Wellenreiter

http://www.wellenreiter.net/

Wellenreiter is a wireless network discovery and auditing tool. Prism2, Lucent, and Cisco based cards are supported. It is the easiest to use Linux scanning tool. No card configuration has to be done anymore. The whole look and feel is pretty self-explaining. It can discover networks (BSS/IBSS), and detects ESSID broadcasting or non-broadcasting networks and their WEP capabilities and the manufacturer automatically. DHCP and ARP traffic are decoded and displayed to give you further information about the networks. An ethereal/tcpdump-compatible dumpfile and an Application savefile will be automaticly created. Using a supported GPS device and the gpsd you can track the location of the discovered networks. NO!, hosap drivers actualy don't work in the perl version.

WIFIscanner

http://sourceforge.net/projects/wifiscanner/

Just another passive 802.11b scanner. It can dump traffic in realtime (like tcpdump) and you can change interactively the sniffed channel. Work with Cisco card and Prism card (with linux-wlan-ng and hostap driver).

AirJack

http://sourceforge.net/projects/airjack/

AirJack is a device driver (or suit of device drivers) for 802.11(a/b/g) raw frame injection and reception. It is ment as a development tool for all manor of 802.11 applications that need to access the raw protocol.

WifiScanner

http://www.hsc.fr/ressources/outils/wifiscanner/

WifiScanner is an analyser/detector of 802.11b stations and acces points. It can listen alternatively on all the 14 channels, and write packets information in real time.

WaveStumbler

http://www.cqure.net/tools.jsp?id=08

WaveStumbler is console based 802.11 network mapper for Linux. It reports the basic AP stuff like channel, WEP, ESSID, MAC etc. It has support for Hermes based cards (Compaq, Lucent/Agere, ...) It still in development but tends to be stable.

Ethereal

http://www.ethereal.com/

Ethereal is used by network professionals around the world for troubleshooting, analysis, software and protocol development, and education. It has all of the standard features you would expect in a protocol analyzer, and several features not seen in any other product. Its open source license allows talented experts in the networking community to add enhancements. It runs on all popular computing platforms, including Unix, Linux, and Windows.

B.2 Malicious Cracking Tools

WEPCrack

http://wepcrack.sourceforge.net/

WEPCrack is an open source tool for breaking 802.11 WEP secret keys. This tool is is an implementation of the attack described by Fluhrer, Mantin, and Shamir in the paper "Weaknesses in the Key Scheduling Algorithm of RC4"

While Airsnort has captured the media attention, WEPCrack was the first publically available code that demonstrated the above attack. We released code and announced to bugtraq on Aug 12, 2001. Airsnort released code about a week later, but had a much more useable and complete implementation for both collection and cracking. Adam Stubblefield and AT&T had the first publically announced verification of the attack, but did not release their source code for public review and use.

LEAP crack

http://www.thc.org/releases.php

THC LEAP Cracker Tool suite contains tools to break the NTChallengeResponse encryption technique e.g. used by Cisco Wireless LEAP Authentication. Also tools for spoofing challenge-packets from Access Points are included, so you are able to perform dictionary attacks against all users.

THC-WarDrive

http://www.thc.org/releases.php

THC-WarDrive is a tool for mapping your city for wavelan networks with a GPS device while you are driving a car or walking through the streets. It is effective and flexible, a "must-download" for all wavelan nerds.

B.3. Reference Sites

http://wiki.personaltelco.net/index.cgi/WirelessSniffer

http://www.linux-sec.net/Wireless/Sniffers/

http://sourceforge.net/

http://wifinetnews.com/