Using Nessus to Detect Wireless Access Points

May 5, 2003
(Updated January, 2009)

Renaud Deraison
Director of Research

Ron Gula
Chief Technology Officer

Table of Contents

Introduction

The detection of wireless access points (WAPs) has become a major source of activity for many enterprise security groups. Conducting physical inspections of each campus location with handheld, laptop computers or even dedicated "wireless monitors" to find unauthorized access points is time consuming. Fortunately, these efforts may be enhanced through detection of WAPs with the Nessus Vulnerability Scanner.

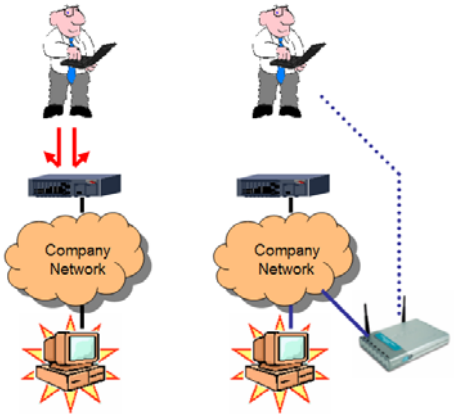
This paper will discuss the techniques used by Nessus to efficiently scan for wireless access points. It will also highlight some of the advantages and disadvantages of scanning with Nessus as compared to manual physical audits. Recommendations for writing signatures to detect new types of WAPs will also be covered.

This paper assumes that the reader is familiar with the Nessus Vulnerability Scanner operating and basic wireless technology. Unless specifically stated, the WAPs that support the 802.11b protocol are assumed.

Why Detect Wireless Access Points?

In campus environments, many network users will add a wireless access point to their network in order to free their laptops and computers from a network cable. In the process of doing this, the network users may be opening the network for unsecured access by remote intruders equipped with wireless network cards. Even though there are simple ways to increase the security of WAPs, many users do not enable these features and this leaves large campus networks exposed to security breaches from remote intruders.

For example, as shown below, a simple corporate network could be protected from the Internet with a firewall. If an internal network user installs an unsecured WAP inside the corporate network, external users may be able to access internal systems.



Simple example of how WAPs can impact security

In the above figure, attacks to breach a server on the "Company Network" are foiled by a firewall. However, with the addition of an unsecured WAP, users outside the firewall are able to access internal systems. Of course, the example may seem to over-simplify the threat of WAPs to network security, but the reality is that war-driving and the plethora of wireless-

ready laptops may expose any internal WAPs to unauthorized network users.

Wireless Scanning for WAPs

WAP audits come in two basic flavors: manual inspection and dedicated inspection.

With a manual inspection, the auditor will configure some sort of mobile device such as a handheld PC or laptop and physically visit the area to be monitored for detection of WAPs. This process can include walking through the area, driving through the area or even flying over the area.

Wireless scanning can occur with active or passive techniques. With an active technique, the auditor will effectively be shouting out a message that says "Is a WAP here?" and look for the "Here I am." response from a listening WAP. This technique typically will find many WAPs, but will not find one that has not been configured to respond to this sort of query. With a passive technique, the mere presence of any wireless communication will be identified. This technique will catch any WAP that is in use, but may not find any traffic if no one is using the WAP during the scan.

For a dedicated wireless monitoring device, it is common to deploy a system that is dedicated to look for WAP activity. These have the benefit of being available 24x7, of being a powerful deterrent and, in the long run, being more cost effective than manual WAP scans. There are a wide variety of open-source solutions available to implement this sort of monitoring as there are commercial tools to monitor the "health" of WAP networks.

Detecting WAPs using Nessus

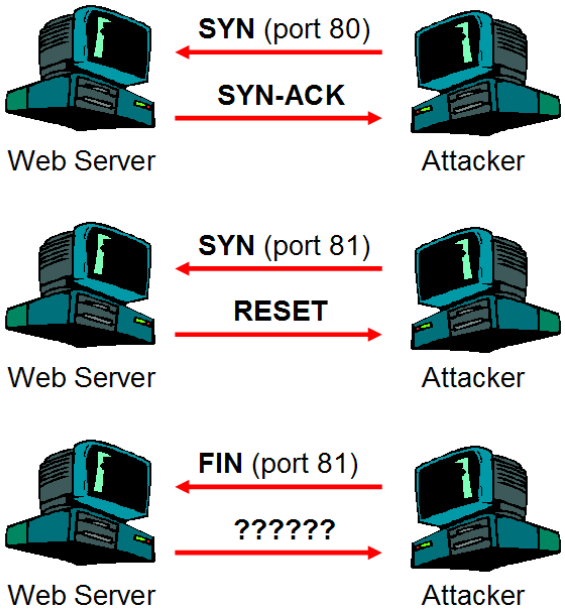
Security auditors attempting to identify the use of WAPs on their networks should consider using a vulnerability scanner such as Nessus that can identify several dozen commonly used WAPs.

The Nessus Vulnerability Scanner is available from http://www.nessus.org/. Its main author and organizer is Renaud Deraison. Nessus performs many security checks for the hosts it tests and these checks are written predominantly in a language named NASL (Nessus Attack Scripting Language). The checks are often referred to as "plugins".

One of the plugins that Nessus uses is ID #11026 and is named "Access Point Detection". It was originally written and submitted by John Lampe. It has since been modified several times to increase the number of different types of WAPs it will detect. The plugin uses four techniques to identify the presence of a WAP. The checks are attempted in series and if one check succeeds, the remaining checks are not executed.

NMAP TCP/IP Fingerprinting

One of the most popular network scanning tools is the NMAP (http://www.nmap.org/) open source project. It performs a wide variety of network discovery and service enumeration techniques. It also has implemented a very popular method for determining the remote operating system based on specific responses from specific TCP/IP probes. Each operating system and network device that speaks TCP/IP attempts to conform to the standards of Internet communication, but there are many undefined possibilities. NMAP can use how an operating system uniquely responds to these possibilities for determining what sort of operating system the target IP address may be.



Fingerprinting via TCP/IP Example

In the above diagram, we show how a remote server may identify the type of operating system that a web server is running. In the first image, we show the start of a TCP session on port 80. All TCP sessions start with a "SYN" packet that lets a client tell a server that it wishes to connect and communicate. If the port is open, the server will respond with a SYN-ACK packet that tells the client that the server can communicate. It is not shown, but typically the client and servers will exchange data and each packet will be marked with an "ACK". When the conversation is done, the client or server can disengage by sending a "FIN" (for "finish") or "RESET" packet. When a port is closed, the rules of TCP/IP state that a "RESET" packet must be sent back to the connecting client.

But what happens when an "FIN" packet is sent to a closed port? Typically, a "FIN" packet is only used when concluding an ongoing TCP session. The rules of TCP/IP state that the correct response is to not have one at all. It turns out though that some operating systems will return a "RESET" packet or some other response. With NMAP, this is a "test".

NMAP attempts around ten different tests like the one above and then compares the results of all tests to a database of known operating system responses. These responses, known as the NMAP Fingerprint Database, are maintained by the NMAP user community.

For WAPs, the NMAP fingerprinting technique is very effective. Even though these embedded devices do not typically run operating systems like Linux or Windows 2000, they do have unique TCP/IP implementations and in most cases, can be fingerprinted. As of the writing this paper, the following NMAP fingerprints can be used to detect WAPs:

```
3Com Home Wireless Gateway
Aironet 630-2400 V3.3P Wireless LAN bridge
Aironet Wireless Bridge running firmware V5.0J
Aironet AP4800E v8.07 - Aironet (Cisco?) 11 Mbps wireless access point
Cisco AIR-WGB340 V8.38 wireless workgroup bridge 340
D-Link DI-713P Wireless Gateway (2.57 build 3a)
```

```
D-Link Wireless Access Point DRC-1000AP - v3.2.28
Linksys WAP11 Wireless AP
LinkSys WAP11 wireless AP firmware v2.2
Linksys BEFW11S4 WAP or BEFSR41 router
Planet WAP 1950 Wireless Access Point
Proxim Stratum MP wireless bridge
SMC Barricade or D-Link DL-707 Wireless Broadband Router
SMC Barricade Wireless Broadband Router (firmware R1.93e)
SMC Barricade DSL Router/Modem/Wireless AP
ZoomAir IG-4165 wireless gateway
```

Nessus plugin #11026 looks into the current knowledge base for the scan in progress and then compares the determined operating system (if there is one) to this list of known WAP TCP/IP fingerprints.

In order to accomplish this type of fingerprinting, at least one port must be reachable by the Nessus Vulnerability Scanner. Also, starting with Nessus 2.0, the TCP fingerprinting functionality of NMAP was re-written by Xueyong Zhi into a standalone plugin written in C named “nmap_osfingerprint”.

HTTP Fingerprinting

Almost every WAP available today comes with some sort of web-based configuration screen. This is very common in the home market and WAP products from D-Link, NetGear and SMC all have similar user interfaces. Each vendor seems to run proprietary embedded web servers on these products and in many cases, they can be identified simply by looking for unique banner information. Here is an example screen capture of the management interface for a D-Link WAP:

D-Link 713P Web Management Interface

There are many items on this screen that could be used to look for a “unique” fingerprint. When choosing a string of information to look for, care should be taken to choose something that will not have any significant false positive rate. For example, simply searching any returned web page for the word “wireless” would not be an effective means of finding WAP web interfaces because the word “wireless” is undoubtedly in a variety of manuals, guides and other web content.

Below is the default HTML returned when making a basic web request to the DL-713P web

management interface:

```
HTTP/1.1 200 OK
Content-Type: text/html
Connection: close

<!---CAS:0003--><HTML><HEAD><SCRIPT LANGUAGE=JavaScript><!--
document.write("<TITLE>")
var l1="713P"
if(l1.charAt(0)=="8")
document.write("multiplex "+l1)
else
document.write("D-Link DI-"+l1)
document.write(" Web Configuration</TITLE>"); //-->
</SCRIPT></HEAD>
<FRAMESET ROWS="60,*,50" BORDER=1>
<FRAME SRC="banner.htm" NAME="banner" MARGINWIDTH=0 MARGINHEIGHT=0 BORDER=1
noresize>

<FRAME SRC="begin.htm" NAME="main" MARGINWIDTH=0 MARGINHEIGHT=0 BORDER=1>

<FRAME SRC="menu.htm?RC=@" NAME="menu" MARGINWIDTH=0 MARGINHEIGHT=0 BORDER=1
noresize>
</FRAMESET></HTML>
```

For Nessus plugin #11026, it was decided to search the returned text from a visited web server for the presence of the string “D-Link DI-”, which is marked in red letters in the above text. Another possible candidate is marked in blue letters that sets a variable for the WAP device version. It could be argued that searching for both strings is more accurate, but being too accurate means that the plugin would not detect versions 713M, 722 and other D-Link products that have not been fingerprinted yet.

Here is another example that came from the Nessus user community:

```
HTTP/1.0 401 Unauthorized
Server: micro_httpd
Date: Fri, 02 May 2003 15:28:57 GMT
WWW-Authenticate: Basic realm="BUFFALO WBR-G54"
Content-Type: text/html
```

In this example, it was decided to add the entire string ‘realm=“BUFFALO WBR-G54”’ to the list of strings searched for by plugin #11026. It is highly unlikely that the string will appear on an audited web page that is not a Buffalo Airstation G54 WAP/Router.

FTP Fingerprinting

In some cases, WAP vendors have added FTP servers to their devices. FTP is mostly used for the uploading of new firmware images when upgrading the WAP device. The banner returned by the FTP service running on the WAP can be used to determine the device’s ID. This is not as popular of a feature though and only two checks (one for a Cisco WAP and one for an SMC WAP) are currently implemented. Unlike the web management interface, keywords like “wireless” and “WAP” can be very effective when used to search FTP banners.

SNMP Fingerprinting

Vendors that want to provide solutions for network enterprises will often include SNMP management in their WAPs so that they can be monitored from Tivoli or HP Openview. If the SNMP port is open and the SNMP community string is also known, plugin #11026 will attempt to probe the SNMP service for the "sysDesc" value. The plugin contains a list of six common access points that can be recognized. Unlike the web management interface, keywords like "wireless" and "WAP" can be very effective when used to search SNMP sysDesc variables.

It is very common to find Cisco WAPs as well as Apple Airports with open SNMP interfaces.

Limitations of WAP Scanning with Nessus

Although the Nessus Vulnerability Scanner is very effective at finding WAPs under the right conditions, the reader should understand when these conditions work against the actual detection of a remote WAP.

Need TCP/IP Connectivity

When conducting the evaluation, if there is no possible way for Nessus to send a packet to the WAP, this technique does not work. WAPs deployed as part of an internal network, extended laboratory network or even a private network that does not have connectivity to the network the scan is originating from, will be ineffective. Similarly, if a WAP is deployed behind a firewall, Nessus will not be able to complete a connection to the WAP in order to identify it.

Disabled PING

A wide variety of WAPs will ship with the ability to disable "ping response" on the WAN network interface. This means that if someone on the corporate side of the WAP attempts to ping the device, the device would not respond. This is important to realize when you configure the Nessus scan. If the scan is relying solely on a scanned host to be "pingable" then WAPs that have this "no ping" feature enabled will be missed.

Could Be Running a Firewall

Many WAPs are now shipped as a one-stop shop for Internet connectivity. They act as WAPs, VPN concentrators and have stateful firewalls built in. If the firewall features are enabled, it is possible to prevent remote connections to the management web interface or potentially, the FTP and SNMP services as well.

Needs a Signature

If a connection does occur to the WAP, the Nessus plugin is configured to detect a specific set of WAPs. If there is a WAP that does not match the current set of checks in plugin #11026, it will not be correctly identified as a WAP device.

Don't know if it is Active

And finally, if a WAP is identified, there may not be any way to tell if the WAP actually has its wireless services enabled. From an auditing point of view, it is likely that WAP devices will creep into corporate networks as they can make excellent HUBs, firewalls and DHCP servers. If SNMP is enabled, it may be possible to walk a set of the variables and see if a

variable is set in such a way that the device's wireless mode can be identified.

Advantages of WAP Scanning with Nessus

Having stated the bad news about scanning for WAPs with the Nessus Vulnerability Scanner, we will now discuss the potential benefits from scanning with Nessus.

Physical Searches Take a Long Time and Don't Occur that Often – Nessus can Scan Every Day

Physical WAP assessments can be very time consuming and expensive. Network users who wish to use WAPs will eventually learn the patterns of the security auditors and implement measures to not be identified by them. If a physical audit for WAPs takes a week to complete, it may be one more quarter before there is another scan.

Completing a Nessus scan on a daily or weekly basis for WAPs is trivial in effort and can offer repeatable tests. For extremely large networks, the results from more frequent Nessus scans can be trended over time.

Less False Positives

A physical search will identify WAPs on the network and off of the network, so there is a potential for the audit to turn up a WAP that is really not part of the network. This would be a false positive. This point should not be taken lightly, as trying to chase down the owners of a WAP in a separate organization may be both politically incorrect and man-power intensive.

Immune to 802.11a, 802.11b and 802.11g "creep"

In 2003, many network WAP vendors have introduced or will be introducing 802.11a and 802.11g WAP technologies. These different layer 2 protocols will complicate passive wireless scanning and make physical assessments to detect all of these technologies more difficult. With the Nessus scan, plugin #11026 simply needs to be updated with the latest signatures of these devices and there is a good chance that the current signatures will detect some of the new equipment from vendors like Cisco and SMC.

Configuring Nessus for a WAP Scan

To conduct a Nessus scan for WAPs, perform the following steps:

1. Perform an update of the Nessus plugins to make sure you have the latest version of plugin #11026. This is accomplished by running the **`nessus-update-plugins`** command.
2. Configure a new scan by selecting plugin #11026 (Access Point detection) in the "General" family.
3. Enable a port scan for ports 1-100. If you want to decrease speed, you could also try scanning ports 21 and 80.
4. Make sure that "Safe Checks" are DISABLED.
5. Make sure that "Enable Dependencies at Runtime" is ENABLED, otherwise OS fingerprinting will break as well as some of the SNMP probes.

Other WAP Identification Techniques

AP Tools

Available from http://winfingerprint.sourceforge.net/aptools.php.

Using Ethernet MAC address identification and a combination of techniques similar to Nessus plugin #11026, this open source solution is able to accurately determine several dozen types of WAP vendors.

Similarly, if you have access to a switch with SNMP capability that also logs the MAC addresses of each device connected to each switch port, you can use a tool like Solar Winds to produce a list of all MAC addresses in use and then search it for known wireless vendors.

Passive Firewall/NAT detection

Packet sniffing tools that watch the sequence of IP packet ID numbers per unique IP address can identify network devices performing NAT translation. Typically, most operating systems will choose a value of one more than the previous IP ID value. In other words, if a sniffer were to watch the packets leaving from a web server, they would have IP ID value of 1000, 1001, 1002 and so on. If multiple computers were using a NAT device, the IP ID values may not change, but the source IP address for all conversations would now have the same ID. An IP ID stream that looked something like 1000, 2000, 3000, 1001, 2001, 3001, 1002, 2002, 3003 and so on could indicate three separate computers access the internet from behind the IP address of the device.

Many WAPs provide DHCP and NAT services to their wireless clients. When these clients share the Internet at the same time, there will be a sequence of IP ID values generated that can be used to identify multiple unique IP addresses behind the WAP. In a large network, it may be feasible to identify all of the router and firewall devices providing NAT services and remove these from a list. What would be left over would be the list of any other NAT device, many of which could be WAPs. This technique will have many false positives, but can ultimately identify all WAPs that are in use.

Conclusion

If you are in the process of conducting a wireless access point assessment of a very large network, then you should try to augment the effort with a network based scan with the Nessus Vulnerability Scanner. This will give you a second set of data that can either verify the results from a physical assessment to find WAPs or possibly identify some WAPs that were not detected during the physical audit.

If you wish to add more checks to plugin #11026, please email either the modifications to the NASL code or the raw information about your WAP device to deraison@cvs.nessus.org.

About the Authors

Renaud Deraison is the primary author and manager of the Nessus Vulnerability Scanner. Nessus has won numerous awards in the computer security industry and from the security community in general. Most recently, it was selected by Network Computing magazine as a winner of their 2002 “Well Connected” award for best vulnerability scanner. It was also

voted as the #1 top computer security tool by the NMAP mailing list, which is made up of many of the leading computer security experts, two years in a row. Renaud is also the Director of Research for Tenable Network Security, Inc. where he continues to develop the Nessus Vulnerability Scanner, conduct security research and work on new computer security products.

Ron Gula is the Chief Technology Officer of Tenable Network Security. TNS is a company that produces the Lightning Proxy for high-speed Nessus vulnerability scans and the Security Center for correlating IDS data with vulnerability data and making it available to multiple people in multiple organizations. Previously, Mr. Gula was the original author of the Dragon IDS and CTO of Network Security Wizards which was acquired by Enterasys Networks. At Enterasys, Mr. Gula was Vice President of IDS Products and worked with many top financial, government, security service providers and commercial companies to help deploy and monitor large IDS installations.

About Tenable Network Security

Tenable, headquartered in Columbia, Md., USA, is the world leader in Unified Security Monitoring. Tenable provides agent-less solutions for continuous monitoring of vulnerabilities, configurations, data leakage, log analysis and compromise detection. For more information, please visit us at http://www.tenablesecurity.com/.

TENABLE Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
TEL: 410-872-0555
http://www.tenablesecurity.com/