tenable network security

Using Nessus to Detect Wireless Access Points

March 6, 2015

(Revision 4)

Table of Contents

Introduction

Over the course of several years, the detection of wireless access points (WAPs) has continued to be a major source of activity for many enterprise security groups. Conducting enterprise-wide inspections of each physical location with laptop computers, or even dedicated "wireless monitors", to find unauthorized access points is time consuming. Fortunately, these efforts may be augmented, and security groups are able to provide a better return on resource investment, through detection of WAPs using the capabilities inherent within the Nessus Professional vulnerability scanner.

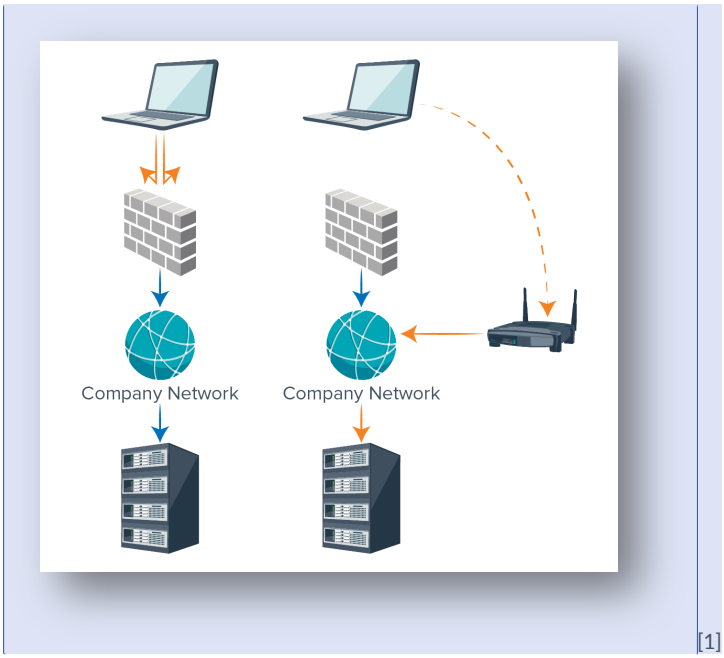
Nessus® is the global standard in detecting and assessing network data. Nessus features high-speed asset discovery, patch and configuration auditing, asset profiling, sensitive data discovery, and vulnerability analysis. This paper will discuss the techniques used by Nessus to efficiently assess environments for wireless access points, and will also highlight some of the advantages and disadvantages of scanning with Nessus as compared to manually performing physical audits.

This paper assumes that the reader is familiar with the Nessus vulnerability scanner and basic wireless technology.

Why Detect Wireless Access Points?

In some organizational environments, users might 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 users may be not only circumventing organizational security policies, but they may also open the network to unsecured access by external intruders equipped with wireless technologies. Even though there are simple ways to increase the security of WAPs, some users do not enable these features, which can increase the risk of leaving their sensitive networks exposed to security breaches from external entities.

For example, as shown below, a simple corporate network is 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.



[1]

Simple example of how WAPs can impact security

In the figure above, attempts 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, this example may seem to over-simplify the threat of WAPs to network security, but the reality is that a plethora of laptops and other mobile

devices, both internal and external to an organization, 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, an auditor will configure some sort of mobile device such as a phone or laptop and physically visit the area to be monitored for the detection of WAPs. This process can include walking or driving through the area, or even flying over the target location (although at relatively low altitudes).

Wireless assessments can be performed through active or passive techniques. With an active technique, the auditor will effectively shout out a message that says "*Is a WAP here?*" and look for the "*here I am*" response from a listening WAP. This technique will typically find many WAPs, but will not find one that has been configured not to respond to this sort of query. With a passive technique, the mere presence of any wireless communication will be identified. This technique will detect any WAP that is available, but may not find any traffic if no one is using the WAP during the assessment.

For a dedicated wireless monitoring device, it is common to deploy a system that is configured specifically 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 well as commercial tools used 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 an active vulnerability scanner such as Nessus, which can identify several dozen commonly used WAPs. Nessus performs many security checks for the hosts it tests.

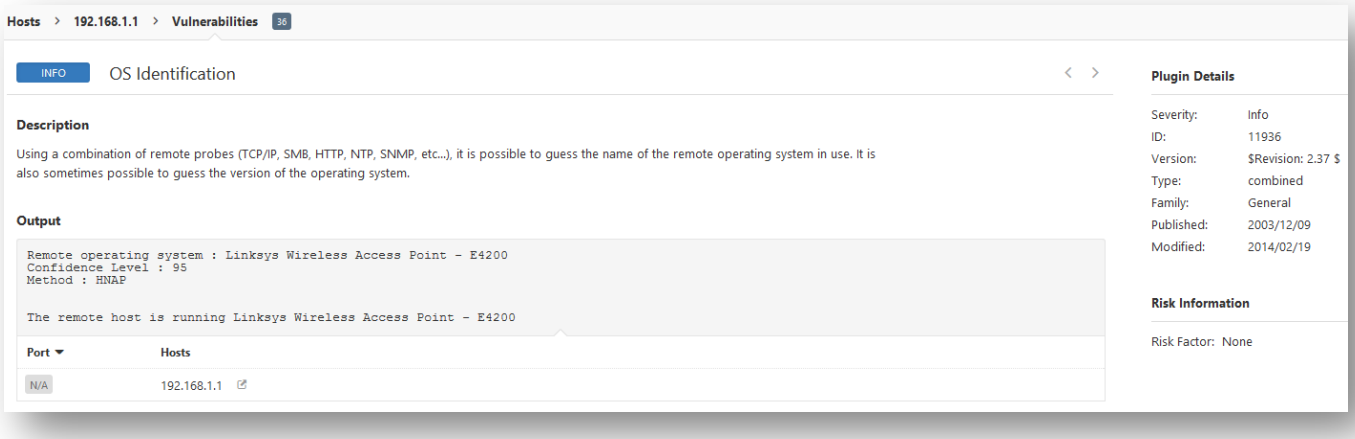
One of the checks that Nessus uses is plugin ID 11026, "Wireless Access Point Detection". It has been modified many times to increase the number of different WAPs it will detect. The plugin uses four techniques to identify the presence of a WAP; the checks are attempted in series and if one check succeeds, the remaining checks are not executed. These techniques involve checking FTP, Telnet, SNMP, and web management interfaces.

Nessus Operating System Fingerprinting

Nessus plugin ID 11936 (OS Identification) is the primary check used to perform operating system enumeration of scanned systems. This plugin takes input from several other plugins, some of which are listed below:

- Plugin ID 35658 (OS Identification : FTP): Uses the remote FTP banner to attempt to identify the underlying OS.
- Plugin ID 35779 (OS Identification : HTML): Uses the HTML content returned by certain HTTP requests to fingerprint the remote OS.
- Plugin ID 25247 (OS Identification : HTTP): Uses the remote web server signature to determine the version of Windows or the Linux distribution running on the remote host.
- Plugin ID 25245 (OS Identification : mDNS): If a mDNS server is present, will perform a highly accurate identification of Apple OS X systems.
- Plugin ID 25248 (OS Identification : MDRPC): Identifies the remote version and service pack of Windows by making certain MSRPC requests against the remote Windows system.
- Plugin ID 25244 (OS Identification : NTP): Queries the Network Time Protocol (NTP) daemon to perform a highly accurate OS guess.

- Plugin ID 25250 (OS Identification : SinFP): Implements the SinFP TCP/IP fingerprinting algorithm. Only requires one open port to fingerprint an OS.
- Plugin ID 25252 (OS Identification : SMB): Identifies the remote Windows OS based on a query to SMB.
- Plugin ID 25246 (OS Identification : SNMP): If credentials are available to perform an SNMP query, data from the "sysDesc" parameter is reported.
- Plugin ID 25287 (OS Identification : SSH): Attempts to identify the remote OS by the SSH banner.
- Plugin ID 29831 (OS Identification : Telnet): Attempts to identify the remote OS by the Telnet banner.
- Plugin ID 25251 (OS Identification : Unix uname): If SSH credentials of the remote Unix host are provided, the results of "uname –a" are obtained.
- Plugin ID 25335 (OS Identification : Linux Distribution): If SSH credentials of the remote Linux host are provided, the specific release will be obtained.
- Plugin ID 25249 (OS Identification : ICMP): This script attempts to identify the OS type and version by sending more or less incorrect ICMP requests using the techniques outlined in Ofir Arkin's paper "ICMP Usage In Scanning".

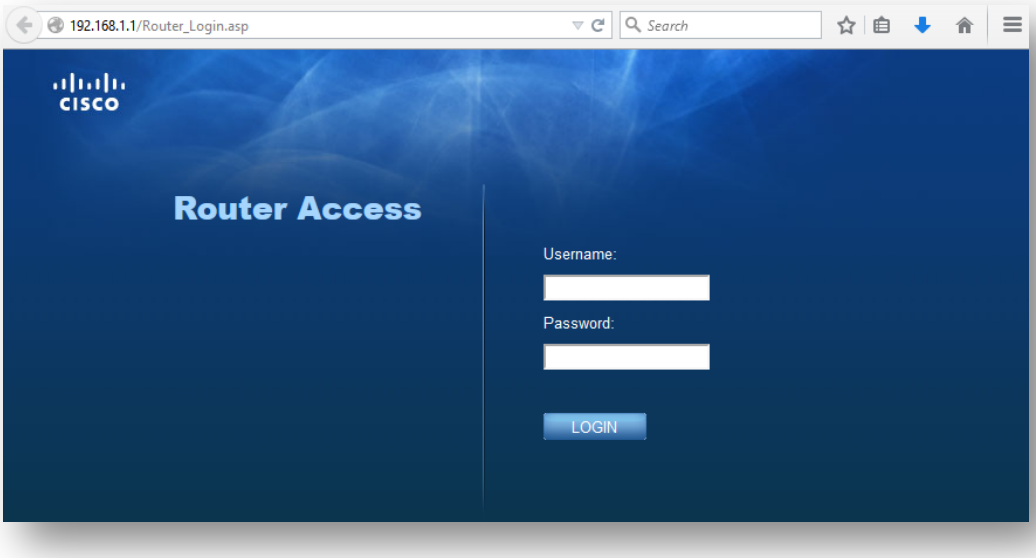


In the screen capture above, an assessment of a local network detected a Linksys Wireless Access Point (model E4200). The Plugin Details show that the identification occurred through plugin ID 11936, and that the HNAP method (via plugin ID 53471 (OS Identification : HNAP)) performed the actual guess that identified the Linksys WAP.

If a WAP is detected using plugin ID 11936 but the operating system, version, or model cannot be guessed, Nessus will then use plugin ID 11026 to perform additional tests to attempt to enumerate the WAP. Nessus plugin ID 11026 looks into the current knowledgebase for the scan in progress and then compares the determined operating system (if there is one) to a list of known WAP TCP/IP fingerprints. In order to accomplish this type of fingerprinting, at least one port must be reachable by Nessus. Additional fingerprinting techniques are listed and described below.

HTTP Fingerprinting

Almost every WAP available today comes with some sort of web-based configuration screen. This is very common in the home market; WAP products from D-Link, NETGEAR, and Linksys 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 Cisco (Linksys) WAP:



Cisco (Linksys) Wireless Access Point Web Interface Login Screen

There are not many items on this screen that could be used to look for a "unique" fingerprint, but 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 a portion of the default HTML returned when making a basic web request to the Cisco E4200 web management interface:

```
 <!--
# Copyright (C) 2009, CyberTAN Corporation
# All Rights Reserved.
#
# THIS SOFTWARE IS OFFERED "AS IS", AND CYBERTAN GRANTS NO WARRANTIES OF ANY
# KIND, EXPRESS OR IMPLIED, BY STATUTE, COMMUNICATION OR OTHERWISE. CYBERTAN
# SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS
# FOR A SPECIFIC PURPOSE OR NONINFRINGEMENT CONCERNING THIS SOFTWARE.
-->
<HTML ><HEAD><TITLE></TITLE>
<meta http-equiv="expires" content="0">
<meta http-equiv="cache-control" content="no-cache">
<meta http-equiv="pragma" content="no-cache">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">


  <style type="text/css">/*<![CDATA[*/
      @import "main.css";
    /*]]>*/</style>
  <script type="text/javascript" src="jquery.js"></script>
  <script type="text/javascript" src="main.js"></script>
```

A possible candidate for fingerprinting is marked in bold letters, and can be used to set a variable for the WAP device manufacturer or version.

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 ID 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. However, this is not as popular of a feature and only a few checks (for Cisco and D-Link WAPs) 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 products such as IBM Endpoint Manager or HP OpenView. If the SNMP port is open and the SNMP community string is also known, plugin ID 11026 will attempt to probe the SNMP service for the "sysDesc" value. The plugin contains a list of several 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 common to find Cisco and HP 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.

Needs TCP/IP Connectivity

When conducting an 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 from which the scan originates, 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.

Ping Disabled

A wide variety of WAPs will ship with the ability to disable a "ping response" on the WAN network interface. This means that if someone on the internal side of the WAP attempts to ping the device, the device would not respond. This is important to realize when you configure a 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 not be detected.

Firewall Enabled

Many WAPs are now shipped as a one-stop shop for Internet connectivity. They act as WAPs, LAN routers, 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 Wireless Access Point Detection plugin is configured to detect a specific set of WAPs. If a WAP does not match the current set of checks in plugin ID 11026 or does not match checks found in the multiple OS identification plugins, it will not be correctly identified as a WAP device.

Unsure if Active

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 may creep into organizational 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 one is set in such a way that the device's wireless mode can be identified.

Advantages of WAP Assessments with Nessus

Having stated some limitations about scanning for WAPs with Nessus, we will now discuss the potential benefits of performing assessments with Nessus.

Frequent Assessments

Physical WAP assessments can be very time consuming and expensive. Network users who attempt to use unauthorized 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 several weeks or months before there is another audit.

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, assessing results from frequent Nessus scans can be trended over time.

Less False Positives

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

Immune to 802.11 version "creep"

Different layer 2 protocols complicate passive wireless scanning and make physical assessments to detect all of these technologies more difficult. With a Nessus scan, plugin ID 11026 simply needs to be updated with the latest signatures of these devices. There is a good chance that the current signatures will detect some of the new equipment from vendors such as Cisco and D-Link.

Configuring Nessus for a WAP Scan

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

1. Perform a Nessus plugin update to make sure you have the latest version of plugin ID 11026. Please refer to the Nessus User Guide (available on the Tenable Support Portal) for instructions on how to perform a plugin update.

2. Configure a new scan by selecting plugin ID 11026 (Wireless Access Point Detection) in the "General" family.

3. Enable a port scan for TCP ports 1-100 and 443. If you want to decrease the amount of time for scanning, you could also try scanning only TCP ports 21, 80, and 443. If other WAP interface and management ports are known (such as TCP 5009 and 10000 for Apple AirPort), include those ports in the Nessus scan policy.

4. Make sure that "Safe Checks" are DISABLED.

Other WAP Identification Techniques

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.

Most 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, you can augment the effort with a network-based scan using Nessus. 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.

About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world's largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, please visit tenable.com.