Global Information Assurance Certification Paper

Bob Konigsberg

GIAC Essentials v.1.2f or 1.3

Auditing Inside the Enterprise via Port Scanning & Related Tools

Summary

This paper assumes that the difficulty of maintaining and verifying the state of all systems on a network of any significant complexity is more than most system/network administrators have time to deal with directly. It proposes that internal port scanning (and derivative tools) be used on an ongoing basis to keep watch on various, listed aspects of network security. A number of commercial, freeware, demo, and open source tools are described along with how best to use them to identify problems. Additional consideration and discussion is given to other planning requirements.

Introduction

It is generally accepted that 80% of the security risks and hazards come from inside an enterprise [1]. Those that start inside (and stay there) can range from forged emails, access to confidential data, compromised machines, which allow for anonymity on the part of the perpetrator. There are also cases where, because of weak perimeter security, outsiders are able to get inside, and then because of internal weaknesses, they are able to compromise more machines.

Given the number of systems in operation at an enterprise of any significant size, it is almost impossible to analyze desktop systems as a group with any manual method. Aside from anti-virus software, which can be set up for automated or semi-automated update and operation, there are few tools to discover weakness on individual systems that are readily deployed to the desktop. Even when IS/IT mandates all configurations, many users bring up "rogue" systems (meaning that IS/IT doesn't know about them). They install unauthorized software, or neglect anti-virus software and patches. The larger the enterprise, the more difficult this is to track. Many organizations are built from acquisitions, mergers and the like and this problem is even more pronounced. There are often conflicting sets of standards. In the case of distant regional offices, controls are sometimes non-existent.

Some smaller or simpler enterprises have never been forced into a disciplined set of policies and practices, and so the general rule is one of chaos.

Many users configure their systems in ways that defeat good security practices simply because it's convenient for them.

Port scanning systems inside the enterprise on a regular basis is one way to keep tabs on several classes of problems; i.e., systems that respond to network requests. This can indicate unauthorized (or worse) software on systems. It is also necessary to help identify

compromised or weak systems. Your organization should develop a method (with management endorsement), of scanning for particular things on a regular basis.

This paper specifically addresses strategies, tactics and methodology, tools and techniques for finding, identifying, and dealing with internal weaknesses through port scanning. Related tools that use similar methods, and tools to resolve the final sources will also be discussed. These tools comprise a mix of freeware, shareware, commercial packages, and techniques using utilities that accompany the operating systems.

Strategy

Identify those weaknesses and compromises that can be exploited over a network, and plan for how you want to deal with them. The list of questions below is a good place to start. Only the first two are expanded upon, as the others are outside the scope of this paper.

Questions to use in planning

- What threats or vulnerabilities should you be looking for?
- How often should you scan?
- How are these to be reported? To whom?
- How will compliance with security standards be enforced?
- What kind of budgeting is available for software and equipment?
- From what location(s) will scanning be performed?

What threats or vulnerabilities should you be looking for? - To effectively address a particular type of threat, you need to know what to look for. Different objectives will require different approaches. First, define what you are looking to learn or find. Each of the areas below will be addressed separately. To aid in planning what to do, the list below represents several classes of potential problems you may want to look at, along with some examples. If you're just getting started, a general search of the network as a whole will help by providing a "picture" of what is out there, thereby allowing you to narrow your focus as needed. Additionally, the list will help point out to management what kinds of threats are out there.

- General Search and Audit – Looking for rogue applications, "back-door" software, worms, accounting of known, identifiable applications.
    - Trinoo (ports 1524, 27444, 27665, 31335, etc.)
    - Back Orifice (port 31337)
    - NetBus (ports 12345,
    - SubSeven (ports 1080, 1234, 2773, etc.)
- Unsecured remote control systems
    - pcAnywhere
    - CarbonCopy
    - Timbuktu
    - LapLink

    - X-Windows
- Identify all Web servers regardless of manufacture (information control)
- Identify and lock down all SNMP capable systems to prevent others from mapping your network.
- Identify open shares with Read/Write or Read Only capability and no security. These can lead to:
    - Access to and compromise of data by others
    - QAZ.trojan - spreads by open shares, infecting NOTEPAD.EXE and opening remote control port. It also attempts to email its originator.
    - W32.elkern.3326 (Open Shares and mapped drives)
    - Allowing others to install software unknown to the user on the system.
- Unauthorized normal servers and/or services
    - IIS 4.0 or 5.0, unpatched can be infected by CodeRed, Nimda and otherwise allow access to system drives. Microsoft no longer supports IIS 3.0, so this should no longer be used.
    - Apache – unpatched can allow systems to be compromised.
    - SMTP Servers without forwarding restrictions can allow your systems to be used to forward SPAM to others.
    - "Private" databases not properly secured
- Unauthorized services/applications that are themselves security risks
    - IRC Servers
    - AIM (AOL Instant Messenger), particularly when not properly configured
- Other worms and viruses that open listening processes or shares to aid in their propagation or notification to their creators.
    - Nimda
    - Future "developments"?

How often should you scan? – As a general rule, *something* (usually a subnet at least) should be scanned at least monthly. This covers general auditing. Scanning for unprotected shares should be done at least once a quarter. Scanning for unpatched servers should be performed as often as possible. Nimda has infected IIS Servers at the author's company within two hours of being installed.

The bottom line here is that scanning should be done on a regularly scheduled basis, since it's difficult to predict what is going to be found on any particular occasion.

Tactics

Scanning for different types of threats will require different tools, or sometimes the same tools used in a different way. Here we explore the same objectives as above, but with an eye toward making effective use of one tool or another, and offer choices where possible.

Is this a general search and audit? Are you looking for rogue software in general? To simply find out generically what kinds of systems and software may be out there, a

default Nmap scan is a good place to start. If you don't have Nmap [7], get it. If you can't run a Unix variant, then use Webfoot's PortFlash product with a ports list that includes TCP ports 1-1024, and the remote control ports for various systems. Systems reporting TCP ports 135 and 139 are generally Windows NT, 2000, possibly XP, and some versions of Windows 98. Systems showing only TCP port 139 are generally Windows 95, 98, or Me. Systems showing TCP ports 21 and 23 (among others) are generally Unix variants. If they are running SAMBA (Unix open software implementation allowing file sharing with Windows systems), TCP port 139 will also show up on the list.

Are you looking for unsecured remote control systems? Symantec's RAPS [8] program is THE tool of choice, followed by Nmap, or PortFlash with a properly configured port list.

Are you trying to find all unpatched versions of IIS? The Retina/Nimda and Retina/CodeRed scanning tools from eEye.com [9] are freeware (in the public service sense of the word), but they are also specific to scanning for their namesakes. However, if a given server responds as not being patched for either one of them, chances are it's not patched for both. The full Retina scanner will look for considerably more than these, but the two released versions do a good job. To find only the unpatched systems, check the box for "Show only vulnerable servers".

Are you looking for all Web servers regardless of manufacture? Same tool as before (Retina/Nimda), but leave the "Show only vulnerable servers" box unchecked. Be prepared to see a lot of web servers used as embedded management tools.

Do you need to identify and lock down all SNMP capable systems? The SolarWinds network discovery tools will query (and build a database) of most of the systems on your network.

Do you need to identify and lock down all unprotected shares (shared folders)? The Legion tool is a good one for building the list of IP Addresses and sharenames. If you want to automatically scan all sharenames to find the writable ones, there is a Perl script at networkeval.com/downloads [7] that will process the Legion list into a batch file that reports writable shares.

Do you need to find the software responsible for opening a listening port on an end station? For systems running Windows NT or 2000 (and possibly XP, not known as of this writing, January, 2002) the freeware command line utility fport from Foundstone will display all listening ports and the application that launched them. TcpviewPro will do the same for all Windows platforms in both a GUI and command-line version. It's not freeware, but it's well worth the money.

Are you having difficult tracking down the physical box in question? So you've got

the IP Address of a suspect system – Now what? To track down a problem often requires that you actually find the machine and/or its owner(s).

Running NMAP –O against the IP address will give you a good idea of what O/S the system is running. In some cases NMAP will get right down to identifying the version and patch levels.

If you don't have NMAP, try performing a ping of the system. Many manufacturers set the ICMP Echo Reply TTL (Time To Live) to different values, and so this is a clue to the general nature of the O/S.

Using PING To Guess at the Type of Operating System

TTL	Nature of Operating System
255	Unix-like systems, routers and many other network devices Macintosh systems also return this.
128	Most Windows systems
64	Nortel (Bay) Contivity, SonicWall SOHO
60	Most Hewlett-Packard JetDirect printers
32	Some versions of Windows 95B/98
30	Sercom Wireless Hub

Note that the TTL will be decremented for each router through which the packet passes. For example, a Cisco router will normally return 255 as a TTL, but you may see 248, meaning that this router is 7 hops away.

Try nslookup or dig to see if the system is in the DNS (Domain Name Service). If you get an answer, see if you can find a TXT record for that system, or contact the DNS admin. Some administrators put the "owner" data in the DNS records directly, and some put the same information in comments in the data files.

If it's a Windows system, "nbtstat –a IPADDRESS" will often identify the workgroup or domain, machine name, and logged in user (if any). Using this data together with the company phone book (or Intranet server) will sometimes lead you to the system's owner.

If it's a Unix or Unix-like system, a telnet, ftp, finger, SNMP sweep will often reveal the name of the machine. If you know the SNMP community string(s) for your organization, that will help in gathering the information you need. If not, then try PUBLIC, PRIVATE, SECRET, SNMP and variations thereof. The tools from SolarWinds.net [3] are particularly useful for collecting any information from SNMP enabled devices.

If you can't find the actual machine (possibly because you don't know what you're looking for), then log into the router or switch, ping the system's IP Address, and then

display the ARP table. Look in the ARP table for the IP address of the machine in question. This will give you its MAC (Media Access Control) – i.e. its Ethernet (or FDDI, or Token Ring, etc.) address. Note the 6-digit (hexadecimal) prefix, without dots or dashes, and point your browser to IEEE OUI and Company ID Assignments [4]. Enter the 6-digit value and click on the Search button. The returned information will often tell you what company manufactured the equipment. This not always accurate because: "***It is important to recognize that this is a partial listing****, as all firms assigned an OUI have not elected to make their official IEEE Organizationally Unique Identifier (OUI) assignment public at this time.*" [4]. However, this gives you a good idea of what kind of equipment you are looking for, and in most cases the OUI and the actual manufacturer match. With a little web surfing and perhaps a call to tech support, you may well be on your way to finding the suspect box. Sometimes tech support can tell you the model of the box and a physical description based on the MAC address.

If none of the above work, and the system is clearly a security threat, there are several ways to isolate and identify the offending machine:

- One dirty trick is to deliberately assign a duplicate IP address to a test machine, or secondary IP address on the router interface. This is often useful for Windows systems (some others as well) because the O/S will put up a message box with an error that can be seen by doing a walk-through of the area where the machine might be located.
- Set up an ACL (Access Control List) on the router to block all traffic to or from that IP address.
- If you have a managed switch on that network, you can also look in the ARP table to find the MAC address of the offending system, and disable that port.
- If you know the port on the switch, a trip to the wiring closet to follow the patch cable may often lead you to the office and jack (outlet) of the offending system.
- If you perform any of the "disabling" options - **Don't forget to notify the help desk to expect that call and to notify you.**

What to look out for (Caveats)

Some legitimate software uses port numbers registered to other software, which can cause false alarms when port scanning. Here are two cases in point. Ports 6667/6668 are used by both IRC (Internet Relay Chat) and APC (American Power Conversion) UPS software. Both NetBus and Trend Micro's OfficeScan use Port 12345. Performing a port scan of your network and finding what appears at first glance to be IRC servers or NetBus can be disconcerting. There are a number of web sites that specialize in tracking odd port numbers. This will be explored in the **Internet Resources** section below.

Heavy port scanning generates a lot of traffic. This can have an adverse effect on WAN links. It can effectively disable some slow links. Additionally, port scanning can sometimes exhaust resources on the scanning machine itself, causing either a system crash or worse (because it's misleading) false negatives, which can lull you into a false

sense of security. It is usually preferable to perform the scanning outside normal business hours.

Many port numbers in use are simply not registered, as opposed to the APC example above where the IRC ports are used, and finding out what software is using them is time consuming.

In the worst cases, port scanning has been known to either crash systems, or render some services inoperable without bringing down the entire system. This is particularly true when systems have not been kept up on patches designed to correct this type of flaw, and the scanning process, especially when it covers many or all ports, simply exhausts the resources of the targeted systems. In some cases (pcAnywhere for example) scanning with RAPS (explained below) has disabled the listening ability of pcAnywhere, although without causing any other harm to the system. For this reason, it is advisable to know where and for what you are scanning before you embark on anything ambitious.

Ironically, a certain amount of light scanning is needed to determine this. For example, to find Windows (and SAMBA) systems, just perform a scan for TCP port 139 (NetBIOS). Once you know where (on which subnets) the Windows systems reside, you can limit your searches to that area. You may also find data center servers, but if you've done your homework, you'll avoid those areas without explicit permission.

Tools of Choice

Tools here are divided into two groups; those that can be run over the network, and those intended for use on the target host itself. The former are intended as scanning software to learn about large numbers of systems. The latter are used as forensic tools to nail down listening ports, to find out what software is actually opening them.

The tools listed here are those with which the author has had experience, and favors. A web search of different tool types will turn up more tools. For example, there are many other port scanners and security scanners out there, but those listed serve satisfactorily. Some tools, like RAPS, I've simply never found anywhere else.

Fport (foundstone.com- freeware [2]) – Fport is a command line utility for NT/2000 systems only, which will show opened listening ports and the application that opened them. Foundstone also sells a product called Vision that not only identifies the source of the open port, but also allows the user to kill the application immediately.

HappyBrowser (Doc Holiday & Ganymed/THC – Beta Test software) - This application runs against a web server looking for known weaknesses in server configuration. The resulting report can then be used to "tighten up" the server. It describes itself as "Beta Test" software, but despite searching, there don't seem to be any later versions out there.

Nessus covers a lot more, but this one will run entirely under Windows. You'll have to do some searching to find a copy.

ISS (Internet Security Scanner – Single host and Networked versions) The Single host version is packaged with the Microsoft Windows 2000 Server Resource Kit. It works only on a local host, presumably the system for which the Resource Kit was purchased. It doesn't fall into the port scanning tool category itself. ISS sells a networked version that allows for an agent on each system, and control from a central point [10]. The Resource Kit version can be used as a good demonstration of the capabilities of the tool. ISS Also sells a network scanner [13].

Legion 2.1.1 (Rhino9.ml.org – Freeware. V. 2.1 was shareware, but 2.1.1 has been released with the shareware notices removed). Given an IP address range (up to Class B size), this will scan for, and identify shared folders on scanned systems. It will also allow the user to map drives directly, but what is often more useful is to take the output file and run it through a batch file or script to map a drive to each sharename, attempt to create a directory with an unlikely name (e.g. t3Std1R), and then log the name of the system, and the share for follow-up. CAUTION – A number of copies of these available for download are infected with viruses and back-door software. They can be cleaned, but beware nonetheless. A Perl script that reads the Legion output and produces a batch file to test and log the writable shares is available at www.networkeval.com/downloads [6].

Nessus (www.nessus.org) "*The "Nessus" Project aims to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner*"[5]. This application requires a back-end server that has to run on a Unix-like platform (Linux is fine), and a user application which is available on Unix, Windows, Java, and possibly others. This is an open-source application, so some technical expertise is required to run it. See their web site for a list of the tests it runs.

Nmap (insecure.org - freeware) – Probably the premier freeware port scanning package, and considerably better than many commercial packages used by the author. This will, by default, scan for most ports from 1-1024, and a number of others in the "undefined" range, which will identify software like pcAnywhere, SubSeven, BackOrifice and the like. The only downside for some users is that it must be run on a Unix system. "*Linux, Open/Free/Net BSD, Solaris, IRIX, Mac OS X, HP-UX, Sun OS, and more. Windows support is in beta and we are not distributing binaries yet*." (www.insecure.org [7]). I've seen very few problems from running the default scans (Two known cases are HP-3000's running MPE, and some Solaris systems which were missing a key patch to the IP stack). This tool allows scanning of both TCP and UDP ports, with root privilege required for UDP.

PortFlash (webroot.com [11] – commercial package) - This is a port scanning utility, but only scans TCP ports. It can scan sequential ranges of TCP ports, or the user can edit the portslist.txt file to specify particular ports of interest. One particular application has been

to maintain a port list file with known remote control software ports. The author used this before learning of RAPS to find remote control software.

RAPS (Remote Access Perimeter Scanner -Symantec.com [8] – commercial package – part of Corporate Edition of pcAnywhere). This one is a blessing where you've got users who set up remote access software without any login requirements. This package will detect most commercial remote control packages, and some of the "back door" types like NetBus. In many cases it will also show you which ones are running without a login required. For pcAnywhere itself, the auditor can optionally lock down the system to prevent its use until the user configures it with a logon. The biggest problem with this is obtaining it to begin with. It is sold only with the Corporate Edition of pcAnywhere, which many vendors are unable to obtain. The author had to go directly to Symantec to get it, but it was well worthwhile. The only problems the author has encountered are on systems deliberately configured without a default router and scanned from outside the local network. The RAPS scan disabled the ability to log into the pcAnywhere software running on the system until rebooted and restarted.

RetinaNimda Scan/CodeRedScan (eEye.com – Class C version - Freeware, Class B version – commercial package) – These two packages are stripped down freeware versions of the Retina security scanner from eEye.com [9]. They were released as a public service by eEye Digital Security to allow system administrators to easily identify web servers on their networks that were vulnerable to Nimda or Code Red respectively. An additional benefit is that if the "Show only vulnerable servers" checkbox is unchecked, the user gets a list of all responding web servers on their network (on the indicated port, default 80), and their respective banners where available. One minor caution here is that many printers and other network devices use a built-in web server for administration, so you may see many more "Web Servers" than you expected. However, it's a great way to find all the IIS, Netscape, Apache and such actual web servers.

SolarWinds Network Management Tools (solarwinds.net [3]– commercial package) - This collection of tools covers SNMP mapping of a network (Not a graphical map), building databases of SNMP gathered information. This is very useful in finding "loose" systems. SolarWinds offers an evaluation package of their tool sets. They also have a number of free tools available for download.

Tcpview (winternals.com [13] – commercial package) – This comes with both a GUI and a command-line version. While not free, this utility will allow identification of what application opened a given listening port on all Windows platforms.

WebBug (Cyberspyder.com [12] - freeware) – This is a useful utility for checking suspect web servers. The folks who make the web site crawler "CyberSpyder" give this out as a freebie. Its purpose is to allow the user to submit an HTTP request, and actually see the text returned by the web server. It is also useful for identifying the maker/type of a given

web server where the server doesn't return a simple banner. It also allows the user to construct a more complex request (such as a POST) and submit it to a web server.

Port Identification Resources on the Web

The following web sites offer assistance in resolving port numbers to applications.
www.iana.com/assignments/port-numbers - Provides official port number assignments and is beginning to include unofficial, but well-known ones.
www.simovits.com/trojans - Lists port numbers for many known trojans
http://www.networkeval.com/undocports.txt - Lists undocumented port numbers based on experience and investigation. If a definition is unsure, it is so described.
www.neohapsis.com/neolabs/neo-ports/ - This is intended to be a "mother-of-all-ports" list, and accepts submissions. They also provide a link to treachery.net for individual port lookups.

Bibliography / Sources

1. **www.trusecure.com - HIPAA Articles - The Board Cares**
2. **www.foundstone.com - Forensic Tools**
3. **www.solarwinds.net/**
4. **IEEE OUI and Company ID Assignments**
5. **www.nessus.org**
6. **www.networkeval.com - Downloads**
7. **www.insecure.org**
8. **Symantec.com - Enterprise Security**
9. **www.eeye.com - Research Tools**
10. **www.iss.net - System Scanner**
11. **www.webroot.com - PortFlash**
12. **www.winternals.com**
13. **www.iss.net - Internet Scanner**