Global Information Assurance Certification Paper

Vulnerability Scanning in the Corporate Enterprise

By: Peter Nichols

GSec Assignment Version 1.2e

Introduction:

Most corporate security professionals live in a world where stealth TCP scanning, midnight vulnerability scans and staring at a sniffer in computer room only occurs at the request of the Human Resources department. Contrary to popular belief, clandestine security activities no longer have a place in securing the corporate enterprise. Many IT managers can ill afford to affront IT professionals that are prone to move to another company at the drop of a hat. It is important to keep in mind the ultimate goal, which is to close security holes. Alienating the IT staff will happen readily enough by interrupting them from their daily chores of keeping the business happy.

The appropriate approach to vulnerability scanning in the corporate enterprise is to publish the scanning methodology, and the means to which the vulnerabilities are to be addressed (via risk closure and risk acceptance procedures). This document will cover the scanning methodology. I encourage its (tailored) publication in any business environment. Make sure everyone on the IT staff and all appropriate business partners fully understand the process. They do not have to understand the mechanics, and it's not necessary to publish those parts. Before any scanning takes place, make sure to have a Security Policy and a Risk Closure/Acceptance methodology in place and published. I will show how these documents will be necessary to take advantage of all the information that will be gathered by scanning.

The Vulnerability Scanning Methodology presented here takes advantage of the best features of both freeware and commercial scanning tools by splitting the task of vulnerability scanning into two parts: Discovery Scanning and Vulnerability Scanning. A freeware program (I chose NMAP) is used to discover or "target" high-risk machines on the network. Once "targeted" the machine will be subjected to a Vulnerability Scan in stages by the more thorough commercial packages such as ISS's Internet Scanner. This methodology will keep your network from being clogged up by running server checks on your Desktop PCs that constitute the bulk of any corporate network. It also has the additional bonus of making the most out of your Vulnerability Scanner licensing agreements.

Scope:

The processes, programs and procedures are limited to the TCP protocols. IPX, ICMP, or any other exclusively non-TCP device will not be detected using this methodology. Although NMAP can detect both TCP and UDP services, UDP's "send it and forget it" nature is not commonly used for enterprise services.

Vulnerability Scanning Methodology:

Definition: Vulnerability scanning covers two basic tasks.

Discovery Scanning: A discovery of resources on the corporate network is performed, and the result is compared to the list of known resources so that resources not reported to the Security department can be investigated, and risks closed.
Vulnerability Scanning: The process of verifying the current operating system configurations are secure. Vulnerability scans run periodically will be used to improve and keep up to date the corporate Operating System Security Standards.

Process:

A *Discovery Scan* must collect enough information about each resource by IP Number attached to the entire corporate network to identify the type of resource (router, desktop computer, server, network switch, firewall, etc.), its operating system and if it is running a service that management has determined as being an "Enterprise" level service (usually via a security policy). These "Enterprise" services are a concern, as they require appropriate management, disaster recovery, etc. Services such as World Wide Web (WWW), File Transfer (FTP), E-Mail (SMTP and POP3), and Name Services are normally classified as "Enterprise" services because they are inherently risky or have a large impact on the corporate network. A full list of services considered "Enterprise" services is included in Appendix A.

- An *Inventory Scan* is the first half of a Discovery Scan. This scan will provide information about the target systems, which can be used to identify the operating system, and the list of ports that the device can be connected to. Often an Inventory Scan will produce enough information on some types of resources that no further discovery will be needed.

- *Classification* is the last half of discovery scanning. This process will identify any applications running on the target system. The applications running on the target system will almost always identify what the resource is (desktop, router, server, etc.).

A full *Desktop Vulnerability Scan* of the standard corporate desktop configuration must be accomplished periodically. This scan ensures that the standard used on corporate desktops is kept current with the latest security patches and software.

A full *Server Vulnerability Scan* will determine if the server operating systems have been configured to the corporate standards, and that applications are kept current with the latest security patches and software. Additionally, all services must be inspected for configurations that compromise security (such as default usernames, and poor passwords).

The Vulnerability Scan is conducted in three phases:

- A *Compromise Scan* checks for vulnerabilities "that can be used by an unskilled attacker, or a system that is already compromised" (ISS, pg 36).
- A *DOS (Denial of Service) Scan* checks for vulnerabilities "that can be taken advantage of by automated attack tools, or by a moderately skilled attacker" (ISS, pg 36). Denial of Service checks will be performed during this stage of the vulnerability scan. These scans, by their nature, must attack the resource in order to see if it is susceptible. Because this test has the potential to interrupt production business processes, the scan should be submitted to the appropriate Change Control Council. If the council cannot accept the chosen date, a new date may be chosen within one week of the submitted date.
- A *Brute Force Scan* checks for vulnerabilities "that can be taken advantage of by highly skilled attacker, or for signs that a system is not configured correctly" (ISS, pg 36). Verifying the integrity of application passwords and service accounts is performed by repeatedly trying common words. Because this test has the potential to interrupt production business processes, the scan should be submitted to the appropriate Change Control Council. If the council cannot accept the chosen date, a new date may be chosen within one week of the submitted date.

Discovery Scanning Mechanics:

Inventory Scanning Setup:

The nuts and bolts of the *Inventory Scan* are accomplished by using the freeware program Nmap and it's companion graphical interface NmapFE available at http://www.insecure.org/nmap. Nmap will run on most any version of Linux, Solaris, or FreeBSD Unix. There is also a version of Nmap that runs on NT, but without the graphical interface. The command structure is the same, and the appropriate command-line commands will be included in this procedure. The implementation of TCP/IP performs much better on Unix then Windows NT; and Solaris does not carry the "toy" stigma that Linux does. In my case, the business choice to run these scans on a Sun workstation with Solaris version 8 was based on both performance and acceptability to the business.

The installations of the Nmap and NmapFE programs require a development system, or "C" compiler, which is not included with the OS on Solaris (but is included with all Linux distributions I have seen). A GNU "C" complier can be obtained for Solaris from http://sunfreeware.com. Installation for most all Unix packages is a matter of downloading the distribution file to the file-system, uncompressing, and then running the configuration program. Directions for installing and compiling both Nmap and NmapFE are included on the Nmap web site. Finally, create a place on the file-system where completed scans will be placed ("*/home/scanner*" is used in the example).

Note: There is one hiccup in installing NmapFE, and that is that it requires a graphics library not normally included with Solaris (and may not be included in some Linux distributions). Download and install the ***GTK+*** (version 1.2.8) graphics library from http://sunfreeware.com before running the Nmap "./configure".

Executing an Inventory Scan:

Every routable IP address in your network must be scanned. In larger companies, this means scanning 10.0.0.0 to 10.255.255.255 (the reserved Class A), and all Internet addresses the company has assigned to it (usually just a single Class C in most cases). It is better to split this daunting task into two sections, scanning addresses known to exist in your network, and then scanning address that should not be used in your network. The group responsible for maintaining the data communications equipment (switches and routers) should make this information available.

Scanning known sections should be performed a Class C network at a time (256 addresses) so as not to blast a busy network.

1. Login to the Unix machine with root permissions.

2. Launch xnmap (usually installed into "/usr/local/bin" to access the NmapFE graphic interface".

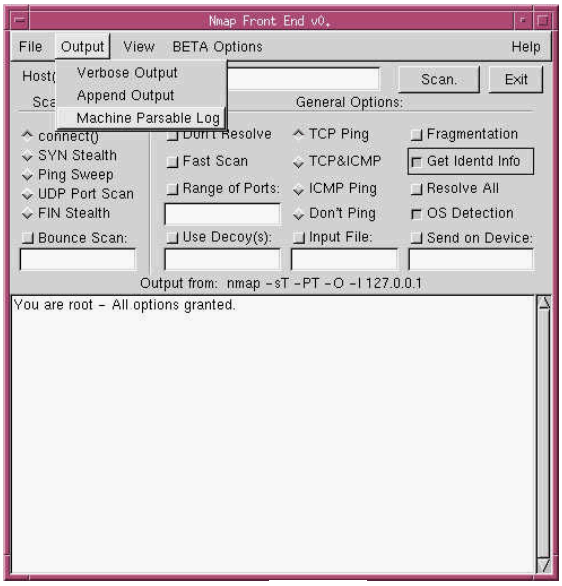


Figure 1

3. Confirm that the **Connect ()** option is depressed. This option is the most compliant and least stealthy of scan modes (see Figure 1).

4. Confirm that the **TCP Ping**, **OS Detection**, and **Get Identd Info** options are depressed (see Figure 1).

5. From the **Output** drop down menu (see Figure 2), click **Machine Parsable Log**. Type "/home/scanner/" followed by the name of the file (use the word "**disc**" for Discovery Scan, the date and an increasing alphabet character as the naming convention (e.g. disc0316a, disc0316b, disc0316c, etc.) and click **Done**.

Figure 2

6. Verify the Output from: field has the correct path and file name. It will now show the command line "*nmap –sT –m **/home/scanner/discXXYYa** –PT –O –I 127.0.0.1*" (see Figure 3).

7. Type the range of the IP addresses to be scanned in the Host(s) field (each Discovery Scan is run for one subnet or one floor at a time).

8. Click Scan. The results of the scan will appear at the bottom of the application box.

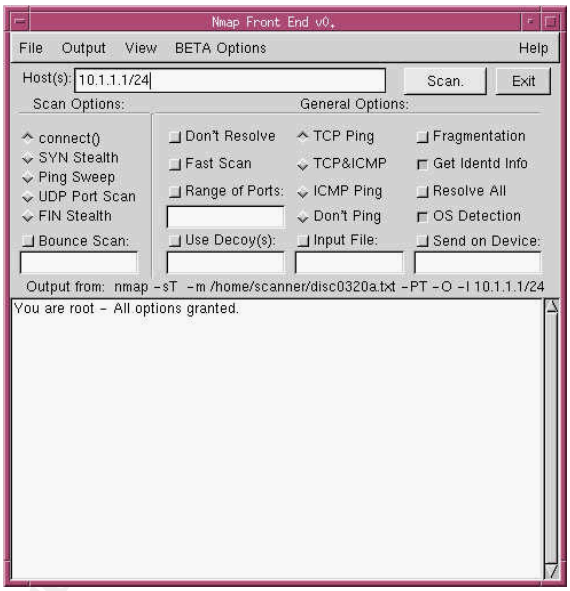


Figure 3

Exporting a Discovery Scan: (not necessary if the scan is run on a Windows NT workstation)

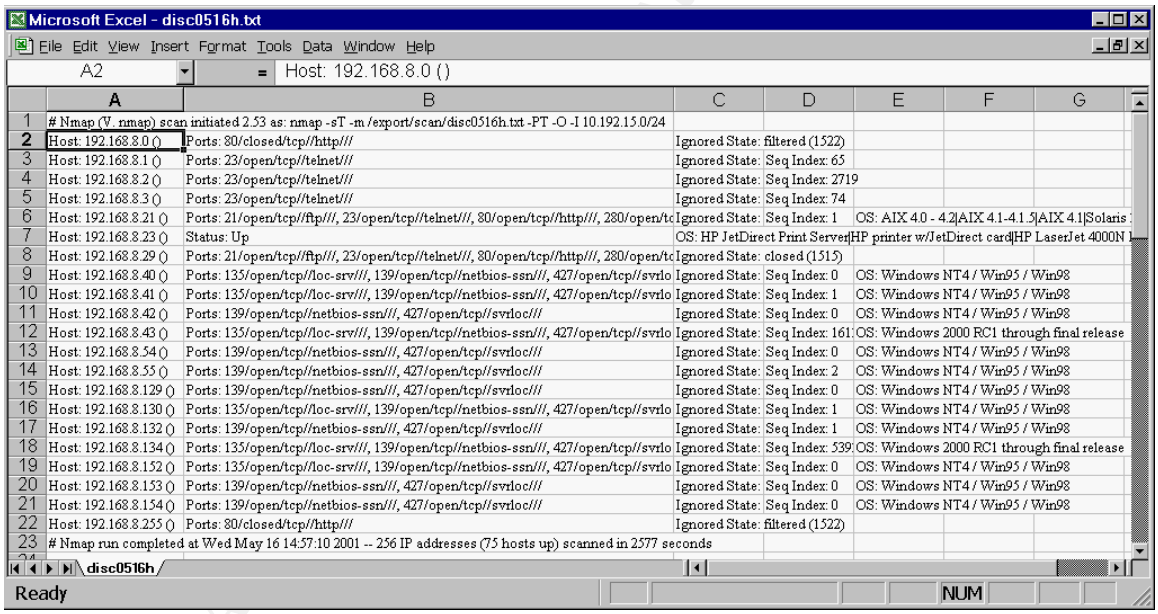
Once the Discovery Scan is complete on the Sun workstation, the report will be exported to a shared drive where it can be reviewed and any abnormal items reported to management. The Sun "FTPD" daemon (server) has to be turned on and your assigned User ID must be removed from the "**/etc/ftpusers**" file. Even though FTP is inherently insecure, it is the easiest to setup and the least impact on the network. Some simple things can be done to limit the risk however, such as removing anonymous access to the server, ensuring that the scan data is never sent across a public (or insecure) network and only running the ftp service when actually transferring scan data.

1. From the Windows Task Bar click *Start*.
2. Click *Run*.
3. Type "Command" in the Open field and click *OK*.
4. Change the local directory to the desired destination of scan output.
5. Type "ftp" and the IP address of the Sun Workstation and press <*ENTER*>.
6. Type in your assigned User Id and press <*ENTER*>.
7. Type your password and press <*ENTER*>. Successful login will
8. Type "*binary*" and press <*ENTER*>.
9. Type "*prompt*" and press <*ENTER*>.
10. Type "*cd /home/scanner*" and press <*ENTER*>.
11. For a single file type "*get* " and the name of file to import and press <*ENTER*>. For multiple files type "*mget* " and the wild-carded name of the files and press <ENTER>.
12. Type "*bye*" and press <*ENTER*>.
13. Type "*exit*" and press <*ENTER*>.

Classification:

The report that is exported from NMAP is reviewed and a report of any abnormal items is compiled for management. This section is where a Security Analyst earns their paycheck, as the results of a scan must be interpreted accurately and a determination must be made as to what's "not normal". In an organized network, similar types of resources will be grouped together so that you could consider a scan with 50 servers and 1 desktop "not normal" although your more likely to see 50 desktops and 1 server (which is probably under someone's desk). The report will essentially require classifying each discovered resource and determining which resources will be targets of further investigation. I can summarize this process by saying that any computer running the services in Appendix A (The Top Dozen Enterprise Ports) should be targeted. Verifying the identity of those targets is a process of opening a web browser, telnet session or ftp client (whichever is appropriate) to that resource.

1. Opening the scan's output file(s) in a spreadsheet application (Microsoft Excel is shown in Figure 4), and adjusting the column size will make abnormal and enterprise services very easy to find.



Microsoft Excel - disc0516h.txt

File Edit View Insert Format Tools Data Window Help

A2 = Host: 192.168.8.0 ()

	A	B	C	D	E	F	G
1	# Nmap (V. nmap) scan initiated 2.53 as: nmap -sT -m /export/scan/disc0516h.txt -PT -O -I 10.192.15.0/24						
2	Host: 192.168.8.0 ()	Ports: 80/closed/tcp//http///	Ignored State: filtered (1522)				
3	Host: 192.168.8.1 ()	Ports: 23/open/tcp//telnet///	Ignored State:	Seq Index: 65			
4	Host: 192.168.8.2 ()	Ports: 23/open/tcp//telnet///	Ignored State:	Seq Index: 2719			
5	Host: 192.168.8.3 ()	Ports: 23/open/tcp//telnet///	Ignored State:	Seq Index: 74			
6	Host: 192.168.8.21 ()	Ports: 21/open/tcp//ftp///, 23/open/tcp//telnet///, 80/open/tcp//http///, 280/open/tc	Ignored State:	Seq Index: 1	OS: AIX 4.0 - 4.2|AIX 4.1-4.1.5|AIX 4.1|Solaris		
7	Host: 192.168.8.23 ()	Status: Up	OS: HP JetDirect Print Server|HP printer w/JetDirect card|HP LaserJet 4000N				
8	Host: 192.168.8.29 ()	Ports: 21/open/tcp//ftp///, 23/open/tcp//telnet///, 80/open/tcp//http///, 280/open/tc	Ignored State: closed (1515)				
9	Host: 192.168.8.40 ()	Ports: 135/open/tcp//loc-srv///, 139/open/tcp//netbios-ssn///, 427/open/tcp//svrlo	Ignored State:	Seq Index: 0	OS: Windows NT4 / Win95 / Win98		
10	Host: 192.168.8.41 ()	Ports: 135/open/tcp//loc-srv///, 139/open/tcp//netbios-ssn///, 427/open/tcp//svrlo	Ignored State:	Seq Index: 1	OS: Windows NT4 / Win95 / Win98		
11	Host: 192.168.8.42 ()	Ports: 139/open/tcp//netbios-ssn///, 427/open/tcp//svrloc///	Ignored State:	Seq Index: 0	OS: Windows NT4 / Win95 / Win98		
12	Host: 192.168.8.43 ()	Ports: 135/open/tcp//loc-srv///, 139/open/tcp//netbios-ssn///, 427/open/tcp//svrlo	Ignored State:	Seq Index: 161	OS: Windows 2000 RC1 through final release		
13	Host: 192.168.8.54 ()	Ports: 139/open/tcp//netbios-ssn///, 427/open/tcp//svrloc///	Ignored State:	Seq Index: 0	OS: Windows NT4 / Win95 / Win98		
14	Host: 192.168.8.55 ()	Ports: 139/open/tcp//netbios-ssn///, 427/open/tcp//svrloc///	Ignored State:	Seq Index: 2	OS: Windows NT4 / Win95 / Win98		
15	Host: 192.168.8.129 ()	Ports: 139/open/tcp//netbios-ssn///, 427/open/tcp//svrloc///	Ignored State:	Seq Index: 0	OS: Windows NT4 / Win95 / Win98		
16	Host: 192.168.8.130 ()	Ports: 135/open/tcp//loc-srv///, 139/open/tcp//netbios-ssn///, 427/open/tcp//svrlo	Ignored State:	Seq Index: 1	OS: Windows NT4 / Win95 / Win98		
17	Host: 192.168.8.132 ()	Ports: 139/open/tcp//netbios-ssn///, 427/open/tcp//svrloc///	Ignored State:	Seq Index: 1	OS: Windows NT4 / Win95 / Win98		
18	Host: 192.168.8.134 ()	Ports: 135/open/tcp//loc-srv///, 139/open/tcp//netbios-ssn///, 427/open/tcp//svrlo	Ignored State:	Seq Index: 539	OS: Windows 2000 RC1 through final release		
19	Host: 192.168.8.152 ()	Ports: 135/open/tcp//loc-srv///, 139/open/tcp//netbios-ssn///, 427/open/tcp//svrlo	Ignored State:	Seq Index: 0	OS: Windows NT4 / Win95 / Win98		
20	Host: 192.168.8.153 ()	Ports: 139/open/tcp//netbios-ssn///, 427/open/tcp//svrloc///	Ignored State:	Seq Index: 0	OS: Windows NT4 / Win95 / Win98		
21	Host: 192.168.8.154 ()	Ports: 139/open/tcp//netbios-ssn///, 427/open/tcp//svrloc///	Ignored State:	Seq Index: 0	OS: Windows NT4 / Win95 / Win98		
22	Host: 192.168.8.255 ()	Ports: 80/closed/tcp//http///	Ignored State: filtered (1522)				
23	# Nmap run completed at Wed May 16 14:57:10 2001 -- 256 IP addresses (75 hosts up) scanned in 2577 seconds						

disc0516h

Ready NUM

Figure 4

2. Create a new spreadsheet (I refer to this as the "Targets" list) to compile all resources that are either enterprise services or where abnormal ports are open. The spreadsheet should contain the IP Number, the Operating System, the DNS or WINS name, the Ports open, a comment field and a "status" field.
3. Notice that the first line of data shows HTTP available on 192.168.8.0. This line can be discounted in this network because a Cisco router or switch is responding to what is essentially an illegal address in this network. Notice that we are getting the exact same response to a broadcast on that network (line

22). The Cisco router's real addresses appear in this subnet at 192.168.8.1-3 (it appears to have three interfaces). How did I know that lines 3,4, and 5 are Cisco routers? I opened a telnet session to that device and got the Cisco standard "User Access Verification" prompt (switches will respond with "Cisco Systems Inc. Console"). Notice that this is listed on line one of the "Targets" spreadsheet.

4. Line 6 shows an AIX or Solaris box at 192.168.8.21. Since this subnet is only supposed to have desktops computers on it, this entry is suspicious. I opened a web browser to http://192.168.8.21 and got an "HP Color LaserJet 4550" banner page. A prime example of why security scan results must be verified.
5. Line 7 shows an HP Laser Jet printer, but no open (TCP) ports. The command "ping 192.168.8.23" returns with a "Request Timed Out". There could be several reasons for this, but since this is a printer I normally list it with a comment of "did not respond to a ping".
6. Line 8 did not return an OS, but opening a browser to that address returned an "HP LaserJet 8150" banner page.
7. Lines 9 to 21 are all Windows desktop computers.

You will not be able to tell whether a desktop is running Windows 95, 98, ME or NT but you can ***almost*** always tell whether it's a desktop or a server by the services it's running. An additional hint is whether the target has a permanent (static) entry in the DNS, the name can also be a tip-off. Finally, have a list handy of servers listed in the NT domain(s). Since all desktops run TCP services 135,139 and 427 any machine running only these services can be ignored. Computers with ports 911, 1001, 1008, 1011, 1012, 1031, or 6712 open are probably running Trojans and should be handled in the same manner as a computer infected with a virus. Any desktop running "Peer Web Services" or running a rouge FTP service will stick out like a sore thumb.

Here are some more examples and how they should be interpreted (the "Ignored State" and "Sequence Index" columns have been removed for clarity):

1. A look at just the ports would lead you to believe that this target is just an ordinary Windows desktop, but it has a static DNS name and the server "FILEZOMBIE" is in Windows Server Manager as a Windows NT Server. This entry definitely deserves more attention.

Host: 192.168.12.130 (filezombie.anywhere.com)	Ports: 135/open/tcp//loc-srv///, 139/open/tcp//netbios-ssn///	OS: Windows NT4 / Win95 / Win98

2. One glance at this entry would make most security analysts cringe. It's accepting SMTP mail, has a web server and can be taken over by PCAnywhere. *Don't panic*, simply add this to the target report making sure to bold and highlight the entry.

Host: 192.168.14.120 (srvtimedev.anywhere.com)	Ports: 25/open/tcp//smtp///, 80/open/tcp//http///, 135/open/tcp//loc-srv///, 139/open/tcp//netbios-ssn///, 443/open/tcp//https///,	OS: Windows NT4 / Win95 / Win98

	465/open/tcp//smtps///, 1030/open/tcp//iad1///, 5631/open/tcp//pcanywheredata///, 65301/open/tcp//pcanywhere///	

3. Although this looks rather innocuous by itself, in a list of 23 Cisco devices this was one of two that had the "finger" port open. It's very likely that this device has been incorrectly or incompletely configured.

Host: 192.168.18.1 ()	Ports: 23/open/tcp//telnet///, 79/open/tcp//finger///	OS: AS5200|Cisco 2501/5260/5300 terminal server IOS 11.3.6(T1)|Cisco IOS 11.3 - 12.0(9)

4. Here's an entry that's the classic "wolf among the sheep". This computer does not have an entry in DNS, and is on a subnet that is supposed to be all desktop computers. The fact that it has port 80 open marks it as unusual. Using a browser returns the banner "Peer Web Services for NT Workstation". One more step can be performed to identify the owner of the computer, and that's looking up the computer's IP number in WINS. Do this by entering the command "*NBTSTAT -A 192.168.20.39*", which will return the computer name and anyone logged into the computer at the time. Note the computer name as the DNS name, and place all logged in ID's in the comments field. This target should be bolded and highlighted.

Host: 192.168.20.39 ()	Ports: 80/open/tcp//http///, 135/open/tcp//loc-srv///, 139/open/tcp//netbios-ssn///, 427/open/tcp//svrloc///, 1030/open/tcp//iad1///	OS: Windows NT4 / Win95 / Win98

5. This workstation is a bit of a mystery, as it does not have any Enterprise services, but the additional port 593 is a bit suspicious. A telnet to this port returns "ncacn_http/1.0". A search of the Internet gives us the following definition of this protocol: "The ncacn_http protocol allows client and server applications to communicate across the Internet by using the Microsoft Internet Information Server (IIS) as a proxy. Because calls are tunneled through an established HTTP port, they can cross most firewalls." Law enforcement would call this "probable cause" and so this computer should be targeted for further investigation.

Host: 192.168.20.157 ()	Ports: 135/open/tcp//loc-srv///, 139/open/tcp//netbios-ssn///, 427/open/tcp//svrloc///, 593/open/tcp//http-rpc-epmap///	OS: Windows NT4 / Win95 / Win98

6. This workstation is not such a mystery, the PCAnywhere program will stand out in any company that uses an Enterprise remote control system for the troubleshooting of it's desktop computers (such as Microsoft's SMS, or Novell's ZEN Works). If your company does not have a policy regarding such programs, then this machine should be targeted for investigation, as PCAnywhere can be quite a security risk when not properly configured.

Host: 10.37.202.4 ()	Ports: 135/open/tcp//loc-srv///, 139/open/tcp//netbios-ssn///, 427/open/tcp//svrloc///, 1031/open/tcp//iad2///, 5631/open/tcp//pcanywheredata///, 65301/open/tcp//pcanywhere///	OS: Windows NT4 / Win95 / Win98

Vulnerabilty Scanning Mechanics:

Vulnerability Scanning Setup:

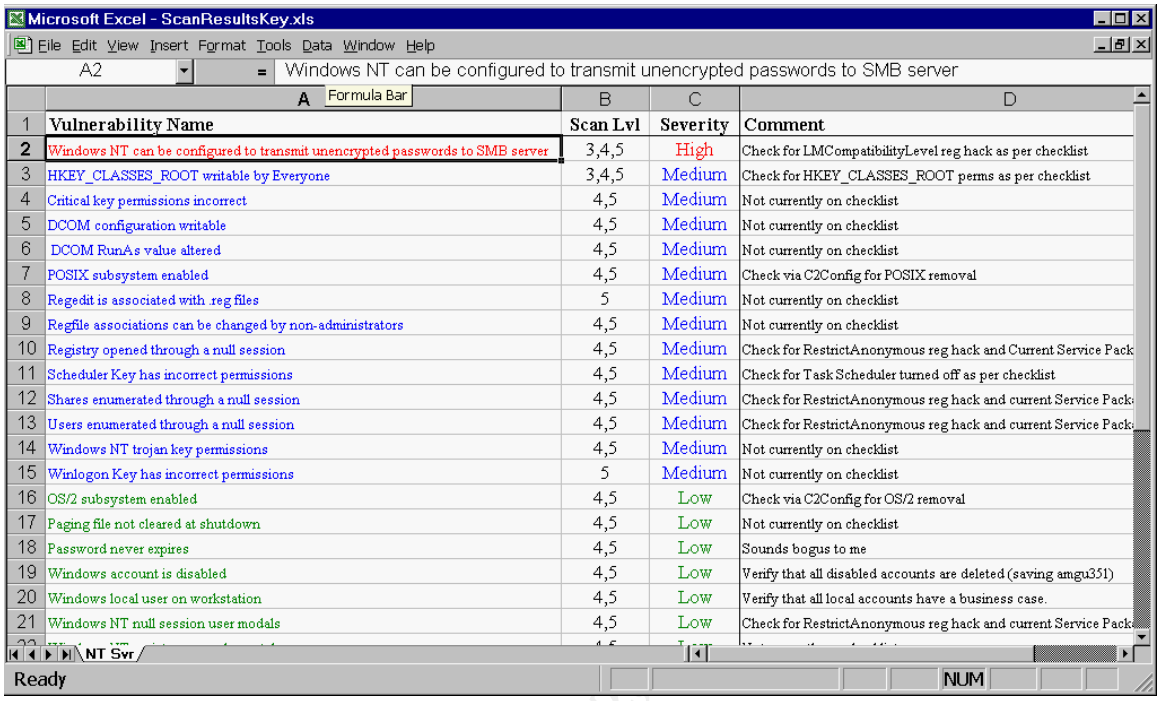
The completion of the discovery scan has produced a definite list of targets to investigate in depth. The following information is based around ISS's Internet Security Scanner, but the methodology will work just as well with any other Vulnerability Scanner. This document will not cover how to setup a commercial scanner (as most are well supported, and all are copyrighted), but will delve into how to go about implementing them into the corporate environment (something they don't teach you in scanner class).

It is important to know exactly what the vulnerability scanner will produce at each stage against a known target. This step is important in avoiding "false-positives" which will cripple the credibility of any report delivered to upper management.

The sure way to understand your vulnerability scans it to run them against a known target. To do this, build a "bare-bones" NT server in an isolated network with all security items normally performed for your network completed. Next perform a Compromise Scan (Internet Security Scanner equates to an "L3 NT Server" template), a DOS Scan ("L4 NT Server") and a Brute Force Scan ("L5 NT Server"); saving a copy of the report for each scan. Compare the "fixes" that the scanner recommends to what has already been preformed on the box, and build a spreadsheet of items to "double-check" at each level of scans.

Most scanners (including Internet Security Scanner) include all tests from a lower level scan in the upper level scans. This methodology will ensure that this is the case, and provides an opportunity to familiarize yourself and your management with the tools in a controlled environment. Like most tools, improper handling can be disastrous.

A sample sheet is shown in Figure 5:



Microsoft Excel - ScanResultsKey.xls

File Edit View Insert Format Tools Data Window Help

A2 = Windows NT can be configured to transmit unencrypted passwords to SMB server

Formula Bar

	A	B	C	D
1	Vulnerability Name	Scan Lvl	Severity	Comment
2	Windows NT can be configured to transmit unencrypted passwords to SMB server	3,4,5	High	Check for LMCompatibilityLevel reg hack as per checklist
3	HKEY_CLASSES_ROOT writable by Everyone	3,4,5	Medium	Check for HKEY_CLASSES_ROOT perms as per checklist
4	Critical key permissions incorrect	4,5	Medium	Not currently on checklist
5	DCOM configuration writable	4,5	Medium	Not currently on checklist
6	DCOM RunAs value altered	4,5	Medium	Not currently on checklist
7	POSIX subsystem enabled	4,5	Medium	Check via C2Config for POSIX removal
8	Regedit is associated with .reg files	5	Medium	Not currently on checklist
9	Regfile associations can be changed by non-administrators	4,5	Medium	Not currently on checklist
10	Registry opened through a null session	4,5	Medium	Check for RestrictAnonymous reg hack and Current Service Pack
11	Scheduler Key has incorrect permissions	4,5	Medium	Check for Task Scheduler turned off as per checklist
12	Shares enumerated through a null session	4,5	Medium	Check for RestrictAnonymous reg hack and current Service Pack
13	Users enumerated through a null session	4,5	Medium	Check for RestrictAnonymous reg hack and current Service Pack
14	Windows NT trojan key permissions	4,5	Medium	Not currently on checklist
15	Winlogon Key has incorrect permissions	5	Medium	Not currently on checklist
16	OS/2 subsystem enabled	4,5	Low	Check via C2Config for OS/2 removal
17	Paging file not cleared at shutdown	4,5	Low	Not currently on checklist
18	Password never expires	4,5	Low	Sounds bogus to me
19	Windows account is disabled	4,5	Low	Verify that all disabled accounts are deleted (saving amgu351)
20	Windows local user on workstation	4,5	Low	Verify that all local accounts have a business case.
21	Windows NT null session user modals	4,5	Low	Check for RestrictAnonymous reg hack and current Service Pack

NT Svr

Ready NUM

Figure 5

Notice how many items show up that I've identified as not being on the standard security checklist, so it's good time to update the checklist. If you don't have a security checklist, then this process will help you build one.

Each type of platform (Windows NT, Windows 2000, Solaris, Linux, AIX, and even your Cisco Routers/Switches) should have a specific documented list of security fixes, and each list should be tested on a regular basis. There will be systems that performing the test scenario may not be possible (tough to get a "spare" AS/400).

Vulnerability Scanning Mechanics:

The *Desktop Vulnerability Scan* can be performed in just the same way as the test server was performed, have the department responsible for desktop support deliver a fully function and "up to snuff" computer to the test lab, and then run a Compromise Scan, DOS Scan and Brute Force Scan, and then build the matrix above. Management will quickly see how "up to snuff" the average desktop is. Always be aware of the culture of the company when representing your results, as too many changes to quickly may cost more in support costs than save in security.

The next step is to mark all targets that do not appear to be servers as "desktop" in the status field. If there are a large amount of desktops that have a specific port open, find out if there is an application tied to that port, so that those desktops do not get targeted in the future. Next, address the targets that have been identified as desktop computers but have services that are not allowed on the corporate desktop. In most cases the

owner of the target does not realize that they have that service running, or they do not realize that the product they are using is not approved for use. Once these services are removed, mark "status" field in the entry on your spreadsheet as "closed".

The desktop computers that are left perform should be treated like a server, as it is now for the security professional to prove that their machine is putting the company at risk. These machines should have a scheduled Compromise Scan and a DOS Scan performed on them, and the report sent to the owner of the computer and the Internal Audit department. . The owner must be invited to sign off on a Risk Acceptance form, at which time the entry in the spreadsheet can be marked as "accepted", along with the date. For those that refuse to sign the Risk Acceptance form, it is important to remember that employees who don't realize (or don't care) how risky their computer is to the network are (as a general rule) are management problems and not security problems. You've identified the risk, and informed the company you work for that the risk is not acceptable.

All that's left on your target spreadsheet is address the servers. Due to the intrusive nature of *Server Vulnerability Scanning*, scheduling of a scan to a specific target should be agreed to by the target's owner, and presented to a Change Management committee. I recommend starting with the Compromise Scan on all targeted servers. The report must then be compared to the target server's configuration. For each exposure uncovered by the report, verify by some other means that the recommended fix has or has not been completed. I usually report all exposures, but include the fact that the fix has already been implemented, but perhaps needs to be re-implemented or that the exposure is a "false-positive" (often the installation of an application will overwrite an OS Patch or security configuration file). Reporting a "false-positive" is only a bad thing when it is not identified as such.

When all vulnerabilities from the Compromise Scan have been addressed, move on to the DOS Scan and then the Brute Force Scan. The philosophy here is to get the vulnerabilities that are easy to exploit closed first, the enterprise will become successively harder and harder to attack. Remember that vulnerabilities "addressed" but not closed will undoubtedly appear in each successive scan.

During the course of this document I discuss "Risk Closure" and "Risk Acceptance". Discovery and Vulnerability Scanning only tell you where your security exposures. It does not tell you what to do when you've found one. My professional experience has taught me that finding security exposures is relatively easy, there are so many! The hard part is figuring out how to close them and why it is important to close them. Before embarking on a Discovery and Vulnerability Scanning program, make sure you have a security policy, publish a risk closure and acceptance methodology, and have a security incident handling system.

Appendix A: The Top Dozen Enterprise Services

The port numbers listed below are by no means exclusive of port numbers that you should flag as being risky, but these ports are the service most abused and have the greatest risk to network.

Port #	Service Name	Service Description
21	ftp	File Transfer Protocol
23	telnet	Telnet virtual terminal
25,109,110 143	Smtp, pop3	Simple Mail Protocol, POP2, POP3 and IMAP Messaging
53	dns	Domain Name Services
80, 443, 8000, 8080	http	Hyper-Text Transfer Protocol, a world-wide web server and any HTTP proxy servers
118	sqlserv	SQL database service
119	nntp	Network News Transfer Protocol
161	snmp	Simple Network Management Protocol
194	irc	Internet Relay Chat
389,636	ldap	Lightweight Directory Access Protocol, an authenticating directory service
2049	nfs	Networking File Systems
5631	PCAnywhere	PCAnywhere Remote Control

Bibliography:

Internet Security Systems. Internet Security Scanner, User's Guide. Atlanta: Internet Security Systems. 2000. 36-39

Fyodor. "NMAP, Free Stealth Port Scanner for Network Exploration and Security Audits." 11 June 2001. URL: http://www.insecure.org/nmap/index.html (18 June 2001)

Sun Microsystems, "Manual Page, in.ftpd." 8 Dec 1999. URL: http://docs.sun.com/ab2/coll.40.6/REFMAN1M/@Ab2PageView/75926?Ab2Lang=C&Ab2Enc=iso-8859-1 (18 June 2001)

Centre for Information Systems Security (DSO National Laboratories, Singapore); Original vulnerability reported by Kalinin, Eugene. "DoS attack against MS Exchange Servers." 21 Aug 2000. URL: http://security.dso.org.sg/forums/windows/messages/10005.shtml (18 June 2001)

Internet Assigned Numbers Authority. "Port Numbers." 16 June 2001. URL: http://www.iana.org/assignments/port-numbers (18 June 2001)

Wallyware, Inc. "NMAP-Services." URL: http://hackerwhacker.com/nmap-services.txt (18 June 2001)

ONCTek LLC. "List of possible Trojan/Backdoor port activity". URL: http://www.onctek.com/trojanports.html (20 June 2001)

Vallabhaneni, S. Rao. CISSP Examination Textbooks, Volume 1: Theory. Schaumburg: SRV Professional Publications, 2000

SANS Institute. "How to Eliminate the Ten Most Critical Internet Security Threats, The Experts' Consensus." 18 January 2001. URL: http://www.sans.org/topten.htm (19 June 2001)

Last Updated: September 26th, 2017

Upcoming Training

Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor