Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Vulnerability Scanners - Tutorial on ISS's System Scanner and a Comparison to Freeware and Commercial Scanners

© SANS Institute 2000 - 2005, Author retains full rights.

GCNT Practical Assignment ver. 2.1
June 26, 2001
By Rae Ward

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Introduction……1
Scope and Intent……1
System Configuration……2
Accounts……2
System Scanner Overview……3
1. Installation……3
2. Vulnerabilities Listing……3
3. General Settings……4
4. System Scanner Policies……5
5. Results……5
Tutorial……6
Part A – Running a Scan Using a Predefined Policy……..6
Part B – Creating and Scheduling a Policy……16
Part C – Monitoring Objects……..21
Drawbacks/Comprehensiveness……24
Comparisons……25
Cerberus' Internet Scanner……25
STAT Scanner 4 with Update 1……26
Description of Features……26
ISS Internet Scanner……28
Description of Features……28
Conclusions……31
Appendix A……33
Appendix B……50
Appendix C……57

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Figures

Figure 1 Source Directory……3
Figure 2 Installing the System Scanner Agent as a Service……3
Figure 3 General Settings Basic Tab……4
Figure 4 General Settings Advanced Tab……4
Figure 5 File Menu……7
Figure 6 Scan Now Window……7
Figure 7 Scan Progress……8
Figure 8 Vulnerability Information……9
Figure 9 Report Menu……9
Figure 10 Vulnerabilities Report Window……10
Figure 11 Report Viewing Options……11
Figure 12 Report Sample……11
Figure 13 Edit Policy Wizard……13
Figure 14 Edit Policy Help……14
Figure 15 Differential Report Window……15
Figure 16 Differential Report Sample……15
Figure 17 New Policy Wizard……17
Figure 18 Schedule a Scan……19
Figure 19 Next Scheduled Scan……19
Figure 20 Command Line Options for Reports……20
Figure 21Processes Baselines……21
Figure 22 File Scan Baselines……22
Figure 23 Initial Baseline Set……22
Figure 24 Object Monitor Results……23
Figure 25 Reset Baselines……23
Figure 26 Baselines Now Reset……24
Figure 27 Cerberus Internet Scanner……25
Figure 28 STAT Analysis Results……26
Figure 29 STAT's Auto Fix……27
Figure 30 FlexChecks……29
Figure 31 File Locations……30

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Introduction

The system administrator's role is to make it as difficult as possible for a hacker to gain access to their systems without hindering the end user's ability to perform their functions. Fixing known software vulnerabilities, setting appropriate permissions on shares and folders, and implementing policies and procedures can help thwart an attack. However, this does not guarantee that a system is hacker proof, because no system is 100 percent secure (Genusa, p. 6). There will always be another unauthorized way into a system – an old vulnerability that remains unfixed, a new exploit, bug, or social engineering. The ability to monitor systems, detect and respond to changes to one's system is paramount (Schneier, p.1). If a hacker can enter your system and remain there undetected, there is no limit to what (s)he can do – create accounts, change permissions on folders or files, delete or alter files, change passwords to lock you out of your own system, alter registry keys - the list is endless. Therefore, to maintain system integrity, some type of monitoring and intrusion detection must also be employed.

The Windows 2000 Server Resource Kit contains System Scanner v.1.1 by Internet Security Systems, Inc., which is a vulnerability scanner. According to the Mitre Corporation, which maintains CVE, the Common Vulnerabilities and Exposures list, vulnerability can be defined as "any fact about a computer system that is a legitimate security concern" (http://cve.mitre.org/about/terminology.html). This can be a bug in the software, weak passwords or account lockout policies. As a vulnerability scanner, System Scanner has the ability to check all these things. Version 1.1 was originally written for NT/9x, so some of the built in bug checks are outdated, but it still proves to be useful on Windows 2000, as we will see, for monitoring objects and checking policy settings.

Scope and Intent

The purpose of this document is to demonstrate how to use System Scanner to detect vulnerabilities by identifying known bugs, checking Windows policies for weak settings and monitoring objects (files, folders, registry settings) for changes. It is not intended to be a definitive document on how to configure a computer to be completely hacker proof, nor is it intended to suggest what settings are appropriate for specifically configured computer (such as a domain controller or web server). It is intended, however, to give the reader some instruction on how System Scanner works, and a basic overview of how to operate System Scanner – how to configure policies, run scans, generate and interpret reports, etc. It is left up to the reader to decide how to best use System Scanner on their computer - what bugs to scan for, how their Windows policies should be set and what objects are important to monitor, all of which will

© SANS Institute 2000 - 2005 Author retains full rights.

depend on the environment the computer is deployed in and what its intended purpose is.

System Scanner will also be compared a freeware scanner, Cerberus, and to two commercial vulnerability scanner products, STAT Scanner and ISS Internet Scanner.

System Configuration

A single system is used in this tutorial, configured as a stand-alone Windows 2000 Professional system as shown below.

Partition Type	NTFS
Operating System	Windows 2000 Pro
Service Pack	None
Computer Name	REMUS
Workgroup Name	Workgroup
Network Protocols	TCP/IP
Software Installed	IE 5.0
	Internet Information Server 5.0
	Office 2000 SR-1
	WinGrab 1.4
	ISS System Scanner 1.1

Table 1 System Configuration

Accounts

As well as the built-in administrator, guest and IIS accounts, two regular user accounts were added to the system. All accounts were left with their default options, as detailed below.

Username	Password	Password Never Expires	User Cannot Change Password	Account is Disabled	Member of
Administrator	newtown	On	Off	Off	Administrators
IUSR_REMUS	YE_xZ3kNUX*1Xo	On	On	Off	Guests
IWAM_REMUS	H8F5d7lpgL&0Aj	On	On	Off	Guests
guest		On	On	On	Guests
johndoe	beautiful	Off	Off	Off	Users

© SANS Institute 2000 - 2005 Author retains full rights.

bobblack	paranoid	Off	Off	Off	Users

Table 2 Account Configurations

System Scanner Overview

1. Installation

To install System Scanner, run sysscansetup.exe from the english\w2kreskit\apps\systemscanner directory on the Server Resource Kit. (See Fig. 1)

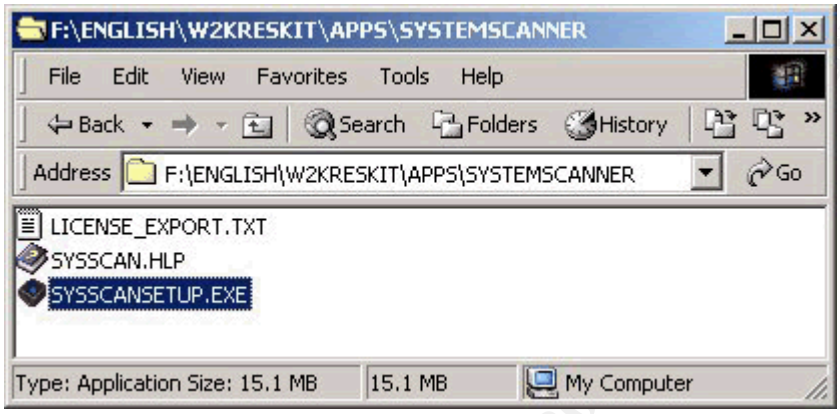


Figure 1 Source Directory

The installation is fairly straightforward – license agreement, destination directory etc. There is a prompt about whether to install the System Scanner Agent as a service (See Fig. 2). If you want to schedule scans to run, without being logged on, you should install the agent as a service. This is recommended. The only reason you shouldn't choose to install the agent as a service is if the system has absolutely no resources to spare.

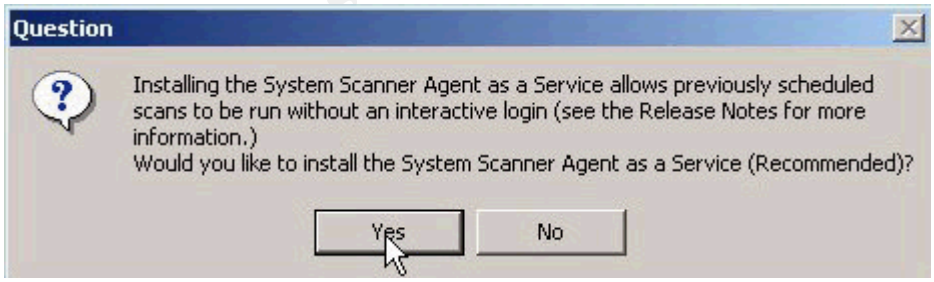


Figure 2 Installing the System Scanner Agent as a Service

2. Vulnerabilities Listing

Once System Scanner is installed, you can get a complete listing of all vulnerabilities that it has the ability to detect for your current setup. Do this by choosing the Vulnerability Listing option from the Help menu. There is a total of 272 vulnerabilities listed that it claims it can detect based on a Windows 2000 installation, but some of these are NT 4.0 exploits or bugs that no longer exist in

© SANS Institute 2000 - 2005 Author retains full rights.

Windows 2000. However, the majority are checks for weak policy settings and change monitoring that applies to both NT 4 and 2000. See Appendix A for the complete listing.

3. General Settings

There are a few general settings that can be configured once System Scanner is installed. These are accessed through the Settings menu, General menu item. The settings on the Basic tab (See Fig. 3) give you the options of having the scans run at low priority in background, and of choosing a scan to run when the system starts, which is only available if the System Scanner agent is installed as a service.

Figure 3 General Settings Basic Tab

On the Advanced tab of the General Settings (See Fig. 4), you can set how long you wish to keep scan results in the database, or choose to purge the database. If you are running scans that produce a large amount of information regularly, you may wish to set this option to less than the 365 day default – it all depends on how much disk space is available, and how long the old scan results are actually useful.

© SANS Institute 2000 - 2005 Author retains full rights.

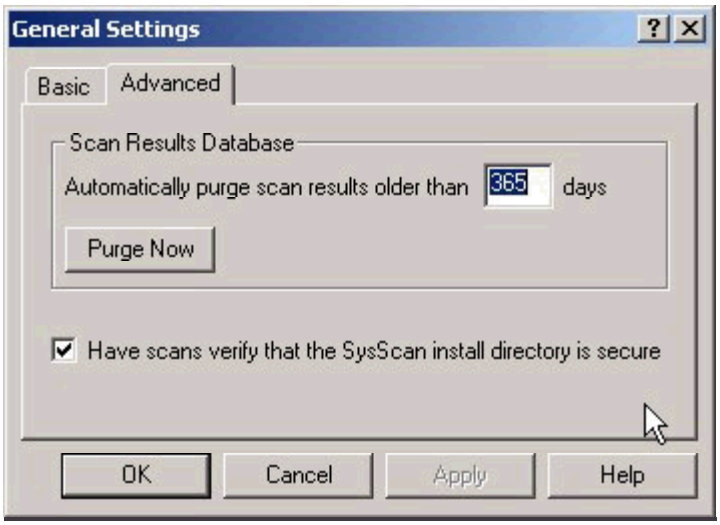


Figure 4 General Settings Advanced Tab

The other option on the Advanced tab is "Have scans verify that the SysScan install directory is secure". The directory that System Scanner is installed in, SysScan, and all its' subfolders and files have NTFS permissions set on them which give the local Administrators and System group full control. If the "Have scans verify…" option is checked, it will check the SysScan folder's and all it's child object's NTFS permissions. If they have changed from the default, they will be set back. For example, if you have a user who is not a member of the Administrators group that you assign read permissions to on the directory where the database of results, db, is kept and you run any scan with the "Have scans verify…" option selected and then check the security on the db directory again, that user will no longer have read permissions.

On the Settings menu there is also a Schedule menu item. This allows you to schedule a scan to be run at a specific time once only, or recurring on any day of the week or any day of the month. This is extremely useful for the forgetful administrator who might not remember to manually run a scan each day.

4. System Scanner Policies

When running a scan, you choose which policy to use. A policy is a group of vulnerability checks that you want to perform on your system. (Not to be confused with Windows Local Security Policy, such as Account policies and Local policies.) System Scanner comes with eleven predefined policies that are tailored to different roles your system may be performing, each with different security levels. For example, there are two policies for desktop workstations, User – Desktop Workstation and User – Power User Desktop Workstation, with the Power User policy checking for more vulnerabilities. Most likely, one of the predefined policies won't contain all the settings required to make your system as tight as possible. In this case you can edit existing policies, or create a

© SANS Institute 2000 - 2005 Author retains full rights.

completely new policy tailored to your needs. Creating and editing policies will be covered in more detail later.

5. Results

After you have run a scan, the results are shown in the Vulnerabilities window, and also stored in the scan results database. Right-clicking on any of the items will bring up detailed information on why the item is flagged as a vulnerability, what OS is affected by it, and how to fix it. All vulnerabilities are also given a risk level of low, medium or high. Table 3 provides an explanation of these risk levels.

Risk Level	Description
Low	vulnerabilities that may provide access to potentially sensitive information
Medium	vulnerabilities that provide access to sensitive data on your workstation, and which may lead to the exploitation of higher risk vulnerabilities
High	vulnerabilities that provide unauthorized access to your workstation

Table 3 Risk Levels

The vulnerabilities found can also be displayed in a report. You can run a report on any scan that is saved in the scan results database. There are four different types of reports to choose from – Vulnerabilities, Services, Trends and Differential.

The Vulnerabilities report contains information on all the vulnerabilities found in one scan, including the vulnerability's description, the severity and a recommended fix.

The Services report lists a summary of Internet services (ex. Finger service) running on the system when the scan ran.

The Trends report allows you to run a report on two or more scans that lists each scan, when it was run, and how many vulnerabilities of each risk level were found. This type of report is useful for determining the progress you are making with eliminating vulnerabilities found during multiple scans with the same policy.

The Differential report takes two selected scans and reports on vulnerabilities in the first scan only (scan with latest time stamp), second scan only (scan with earliest time stamp), common to both or any combination of the three. Running a report on two scans with either vulnerabilities in the first scan only or second scan only options selected would produce a listing of new vulnerabilities to be addressed or vulnerabilities that have been corrected, respectively.

© SANS Institute 2000 - 2005 Author retains full rights.

Tutorial

Part A - Running a Scan Using a Predefined Policy

To get a general idea of how to use System Scanner, this section covers running a scan using a predefined policy, the User – Desktop Workstation policy, on an out of the box Windows 2000 installation, editing the policy, generating reports and interpretation of the results. (Note that there is a quick tutorial in the System Scanner Getting Started Guide in the installation directory. The tutorial that follows is greater in depth and explanation.) For a complete list of all vulnerabilities found by the User – Desktop Workstation policy, see Appendix B.

1. Start System Scanner. This can be done by selecting the System Scanner 1.1 option from the ISS menu item under Programs on the Start menu, or, if System Scanner Agent was installed as a service, double clicking the System Scanner icon in the taskbar.

2. Choose the Scan Now… option from the File menu. (See Fig. 5) This opens the Scan Now dialog box.

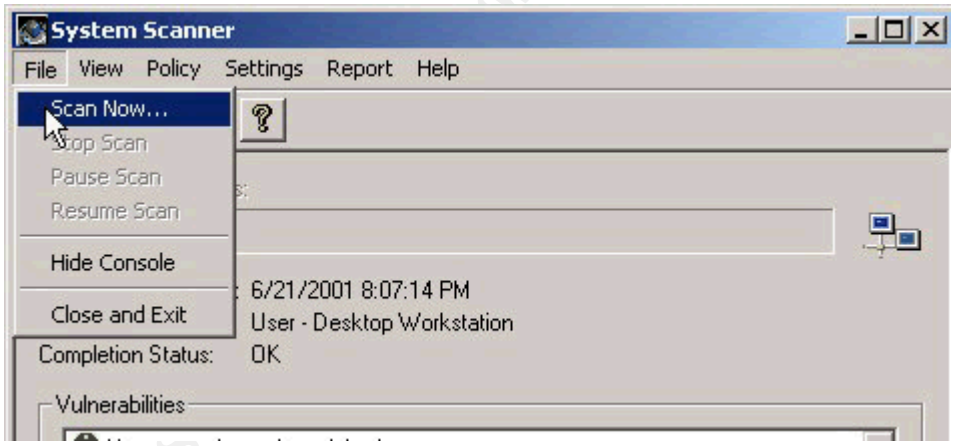


Figure 5 File Menu

3. In the Scan Now dialog box, choose which policy to scan with and, optionally, enter a comment to be associated with the scan. We will choose the User – Desktop Workstation policy for our initial scan and then click on the OK button. (See Fig. 6)

© SANS Institute 2000 - 2005 Author retains full rights.

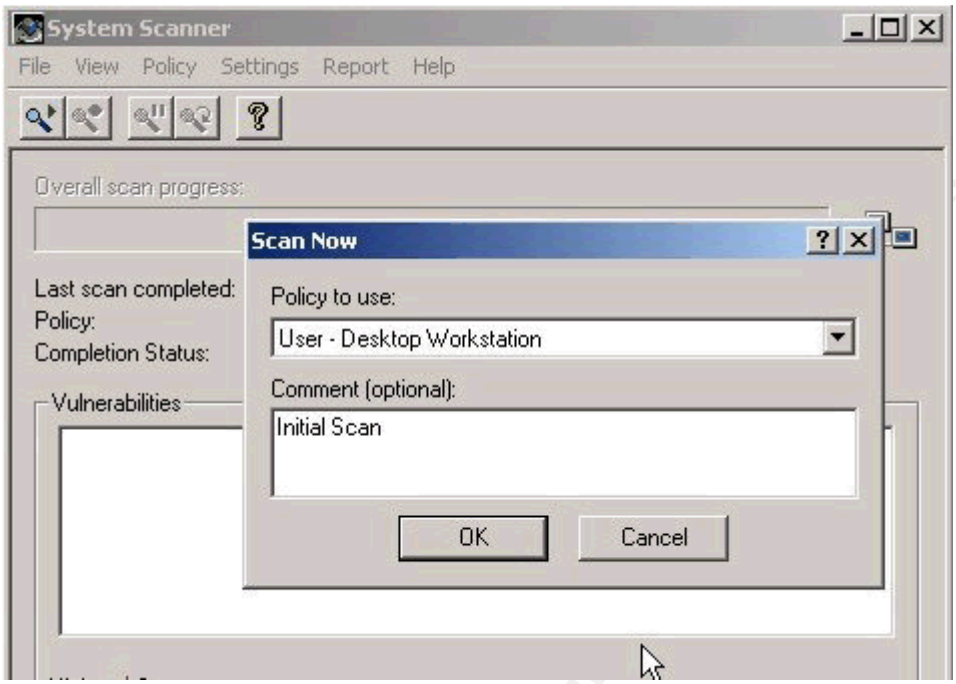


Figure 6 Scan Now Window

4. As the scan runs, the Overall scan progress bar displays the progress of the scan, and the vulnerabilities appear in the Vulnerabilities window as they are found. (See Fig. 7) There are also three vulnerability counters at the bottom of the window displaying how many high, medium and low risk vulnerabilities were found.

© SANS Institute 2000 - 2005 Author retains full rights.

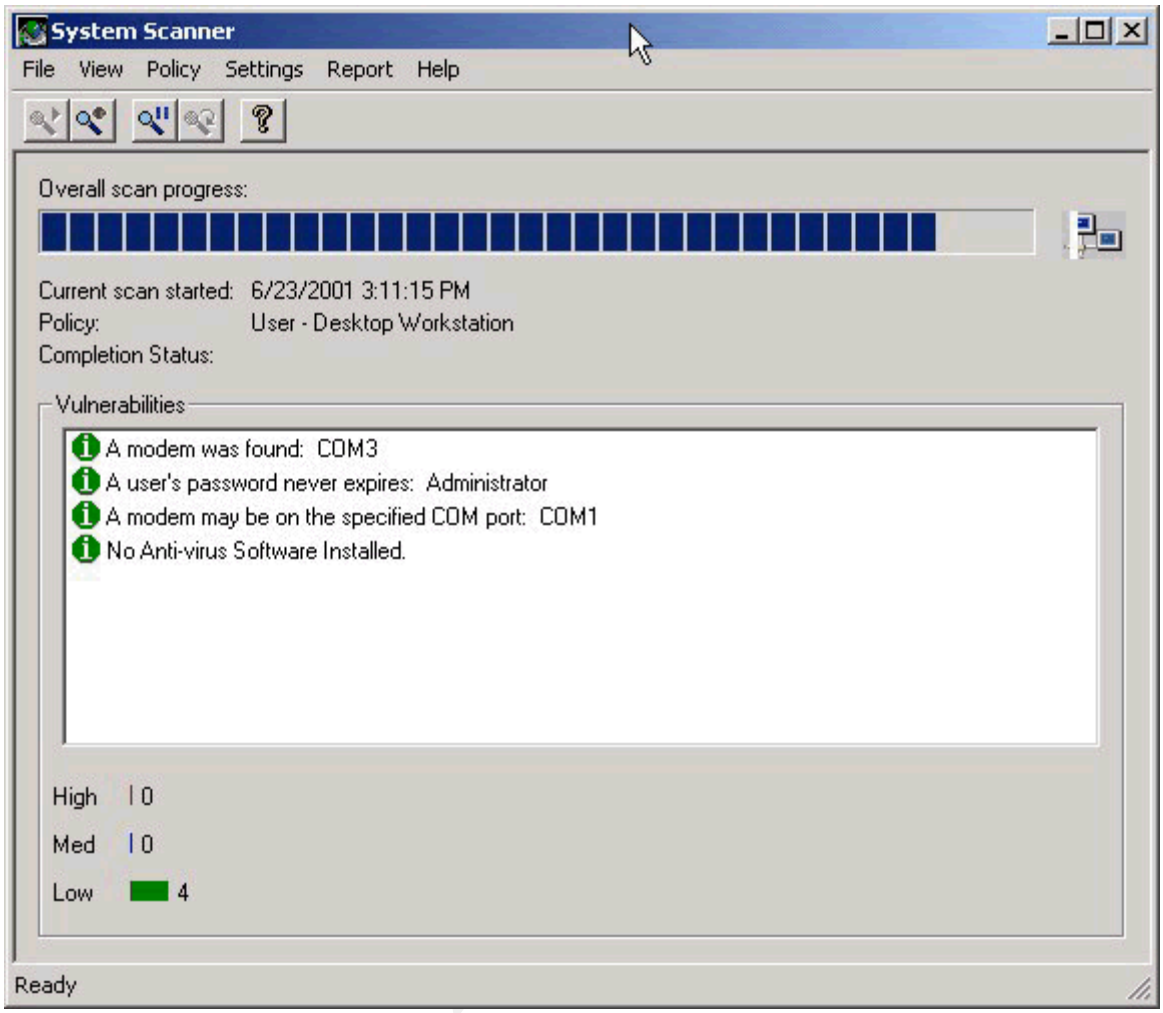


Figure 7 Scan Progress

5. When the scan has completed, right clicking on an item in the vulnerabilities window brings up a detailed help on that particular vulnerability, including why it is considered a vulnerability, the risk level associated with the vulnerability, and a suggested fix for that vulnerability. (See Fig. 8)

© SANS Institute 2000 - 2005 Author retains full rights.

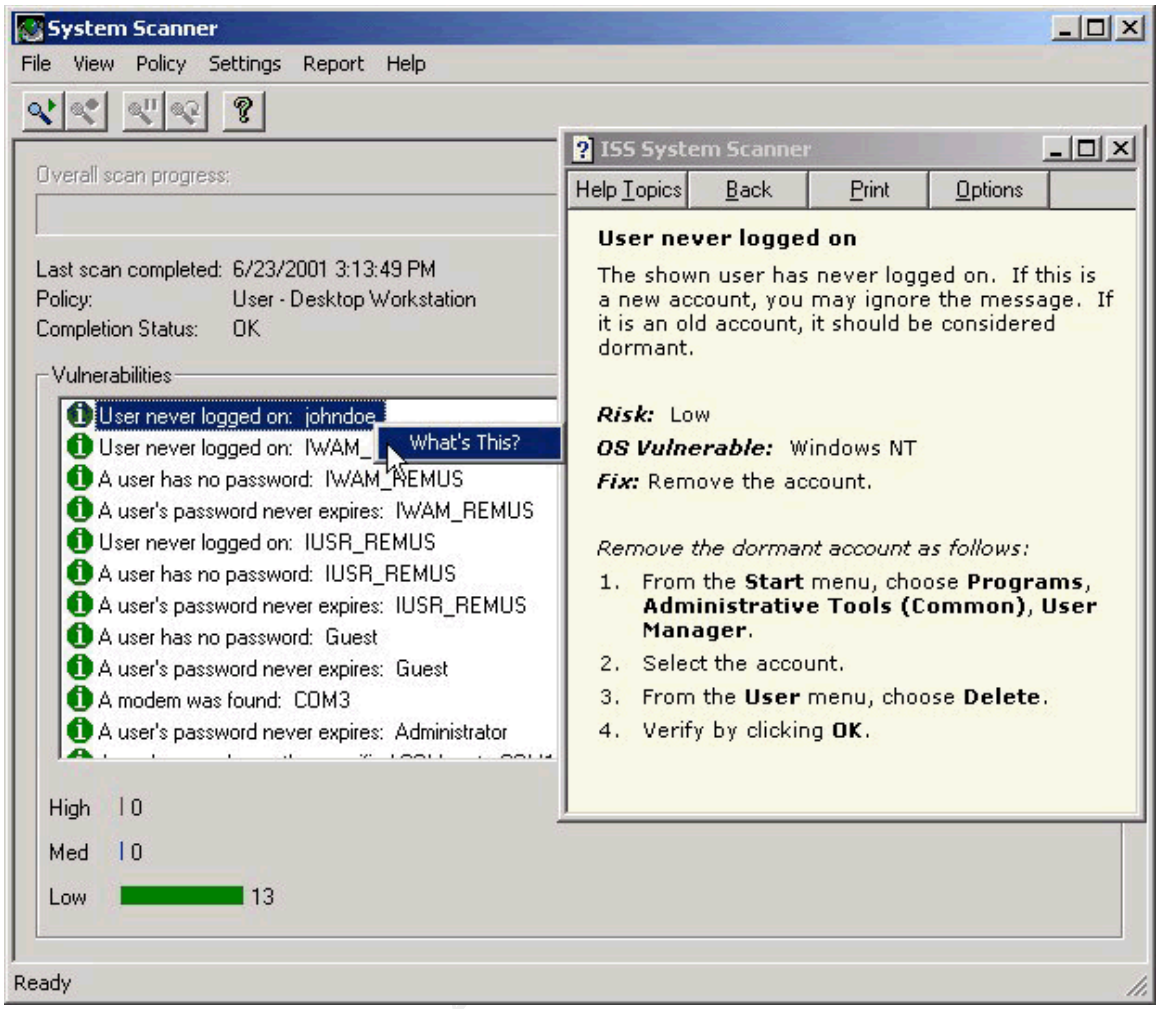


Figure 8 Vulnerability Information

6. Run a report on the results of this scan by clicking on the Vulnerabilities menu item from the Report menu. (See Fig. 9)

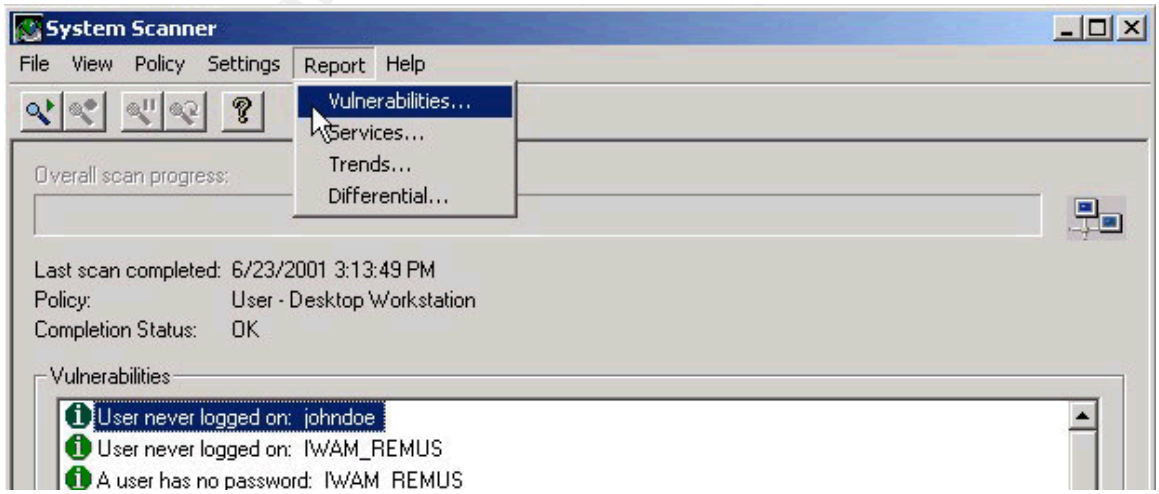


Figure 9 Report Menu

© SANS Institute 2000 - 2005 Author retains full rights.

7. This opens up the Vulnerabilities Report window (See Fig. 10). There are several options here. In the main Scans window choose which scan you wish to generate a report for. Under the Vulnerability Severity heading, you can choose which vulnerabilities you want the report to show based on their risk level. Under the Report Detail heading the Full Description option, if checked, will put in the report a description of why each item found by the scan is considered a vulnerability. If the Fix Information box is checked, the report will contain a suggested fix for each vulnerability. Checking the Scan Policy Info box will add a summary of the policy that was used in the scan to the bottom of the report. Hit the Next button.

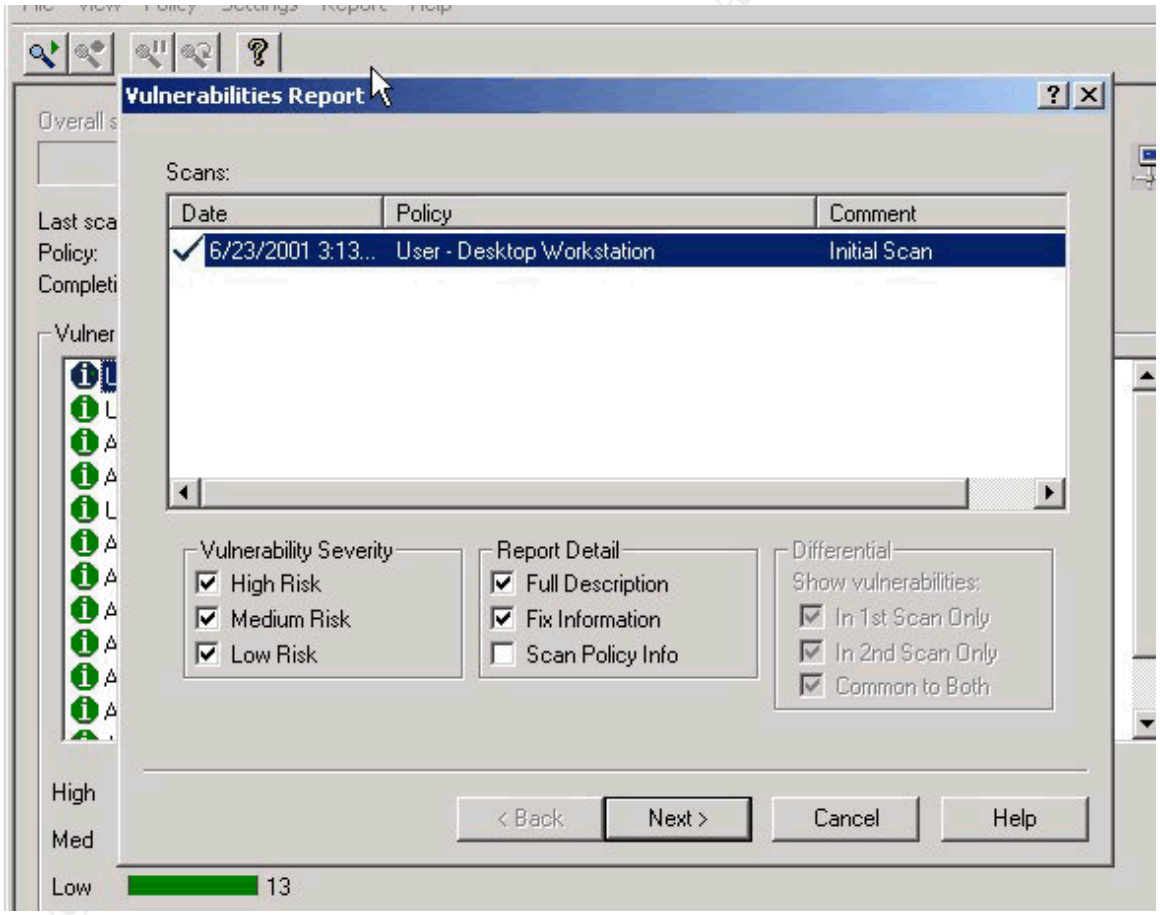


Figure 10 Vulnerabilities Report Window

8. Accept the default of View Report in your Browser. There is also the option of saving the report to an HTML file. (See Fig.11)

© SANS Institute 2000 - 2005 Author retains full rights.

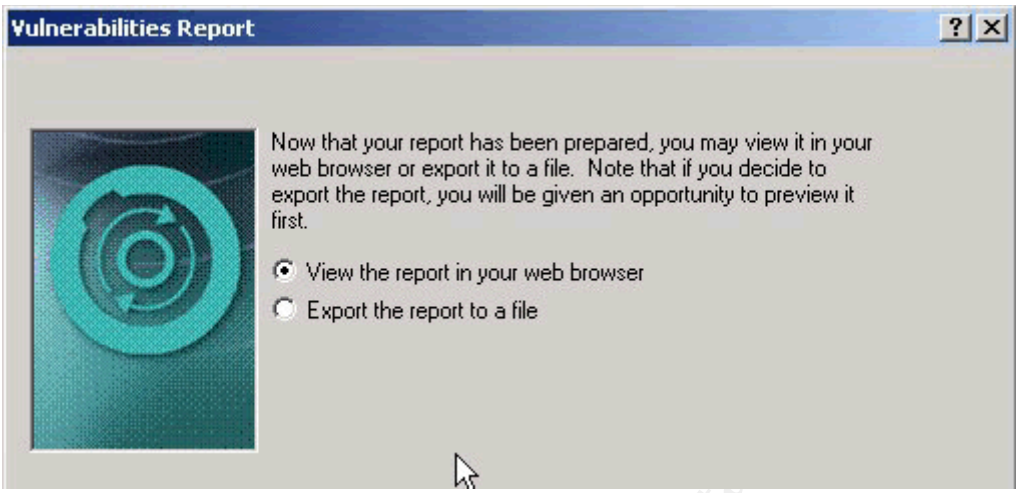


Figure 11 Report Viewing Options

9. The report is generated, showing all the vulnerabilities found by our scan, including a full description and suggested fix for each vulnerability. A sample of the report is shown below. (See Fig. 12) See Appendix C for the full report.

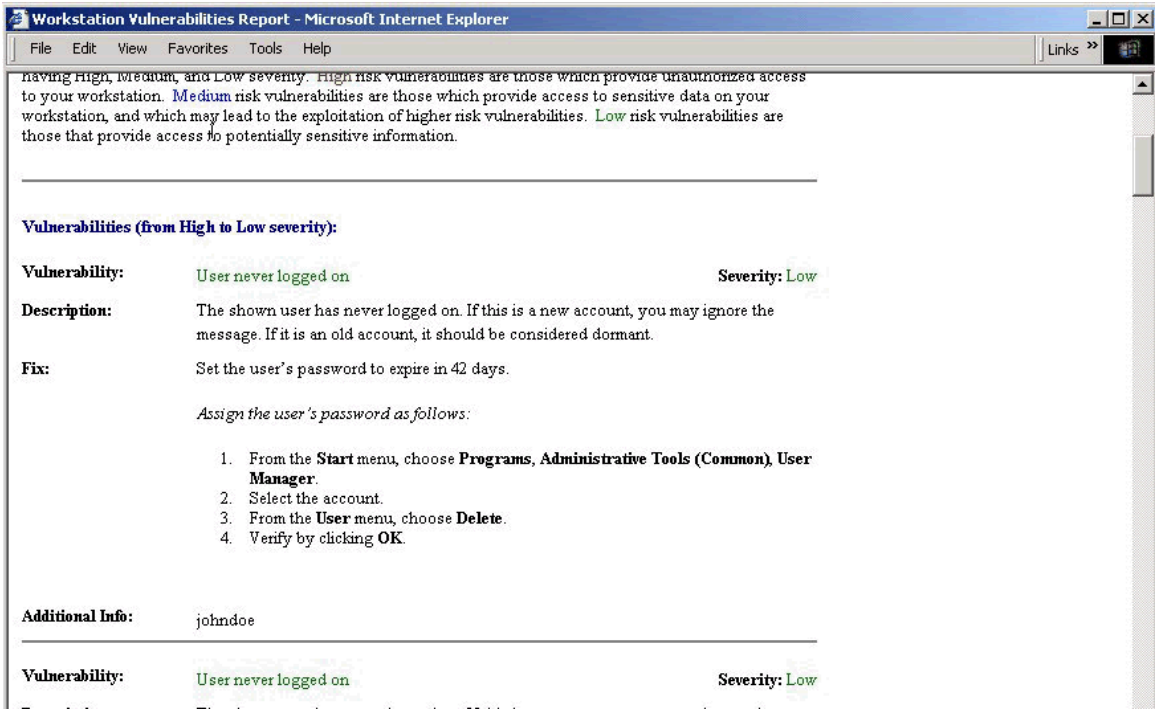


Figure 12 Report Sample

10. Use this report to fix as many of the vulnerabilities as you deem necessary. For example, the scan found a modem on COM3, but no account has dial-in privileges on this computer, so no corrective action will be taken. Also, System Scanner did not detect any anti-virus software installed, but it only checks for Solomon, Norton and

© SANS Institute 2000 - 2005 Author retains full rights.

McAffee, so if you have another anti-virus application installed on your computer (Sophos, Panda and others), this item can be ignored, or better yet, turned off in the policy. The vulnerabilities found and actions taken are shown in Table 4.

Vulnerability	Account	Comment	Action
User never logged on	Johndoe	No problem - new user	None
	IWAM_REMUS	Will be used by IIS – not dormant	None
	IUSR_REMUS	Will be used by IIS – not dormant	None
User has no password	IWAM_REMUS	Account does have password - false result	None
	IUSR_REMUS	Account does have password – false result	None
	Guest	Account is disabled	Set password for guest – if enabled, password won't be blank
User's password never expires	IWAM_REMUS	Used by IIS, allowing it to expire could cause problems with IIS	None
	IUSR_REMUS	Used by IIS, allowing it to expire could cause problems with IIS	None
	Guest	Account is disabled	None
	Administrator	Account should be renamed	Rename account, allow to expire
Modem was Found COM3	N/A	No account has dial in access allowed	Disable checking for modems
Modem may be on COM1	N/A	False result	Disable checking for modems
No anti-virus software installed	N/A	Only checks for certain applications	None installed – leave enabled as a reminder

Table 4 Initial Scan Results and Corrective Actions

© SANS Institute 2000 - 2005 Author retains full rights.

11. After setting the password for the guest account, renaming the administrator account and setting both accounts to expire, we also need to edit the policy to disable checking for modems. This is done by choosing the Edit… item from the Policy menu. In the Policy drop down list (See Fig. 13) choose the User – Desktop Workstation from the menu list, and accept the default of Let me choose all settings for myself, then click Next.

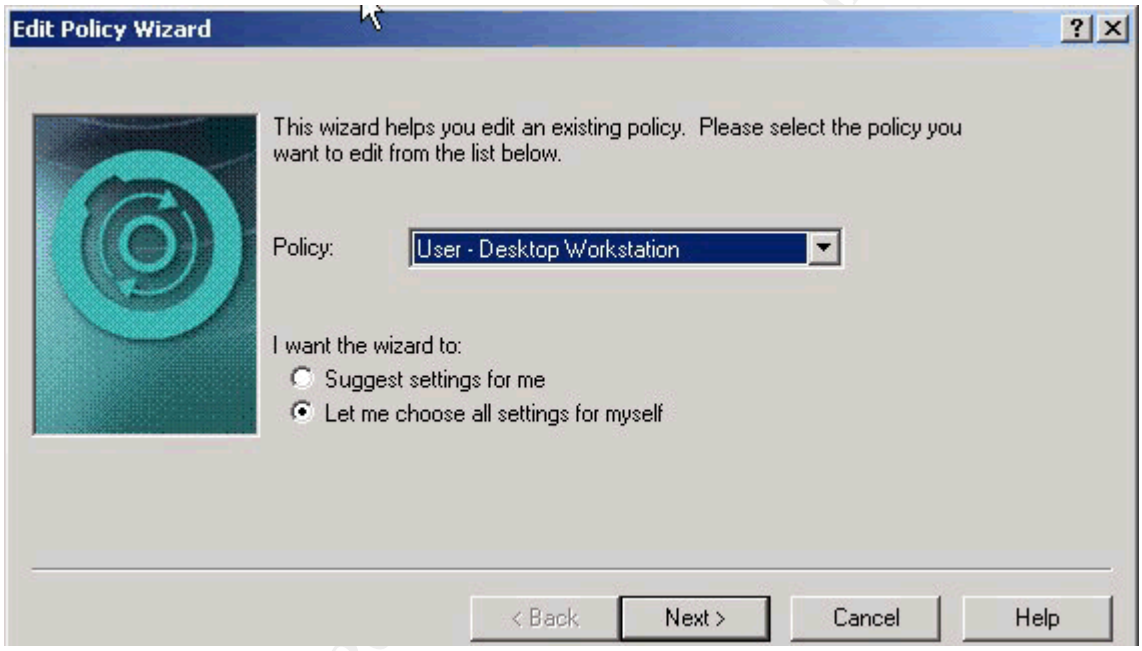


Figure 13 Edit Policy Wizard

12. The Edit Policy Wizard window opens (See Fig. 14). Here you can turn on or off any of the built-in checks, as well as put in settings for those checks that require them. Turn off the check for modems by clicking on the plus sign beside Remote Access to expand the topic. Click once on the check mark beside Modems to deselect it. As seen before, right clicking on any of the groups brings up a description of that particular vulnerability check. Click on Finish to save the changes made to the policy.

© SANS Institute 2000 - 2005 Author retains full rights.

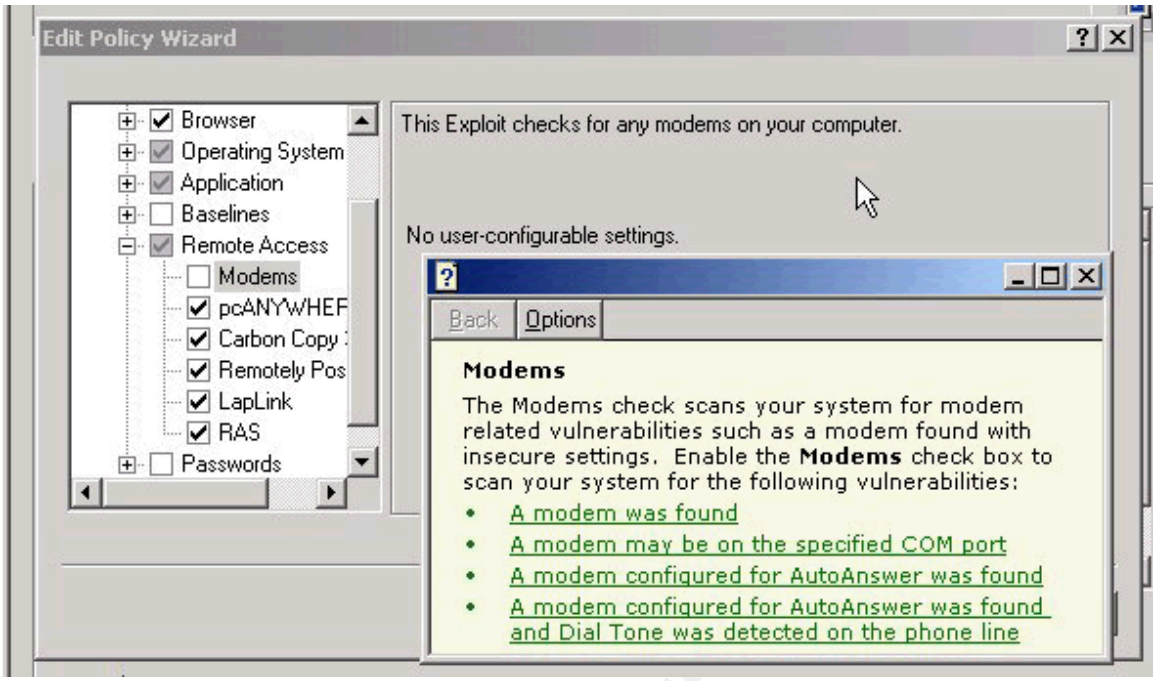


Figure 14 Edit Policy Help

13. Run the modified User - Desktop Workstation policy by following steps two and three above.

14. Generate a report to find out which vulnerabilities no longer exist, and to check that no new vulnerabilities were introduced. From the Report menu, choose Differential…

15. In the Differential Report window (See Fig. 15), select one scan, hold down the Shift key and click on the other scan so that both are highlighted. In the Differential box, uncheck the Common to Both option. Click Next, and then Finish to generate the report.

© SANS Institute 2000 - 2005

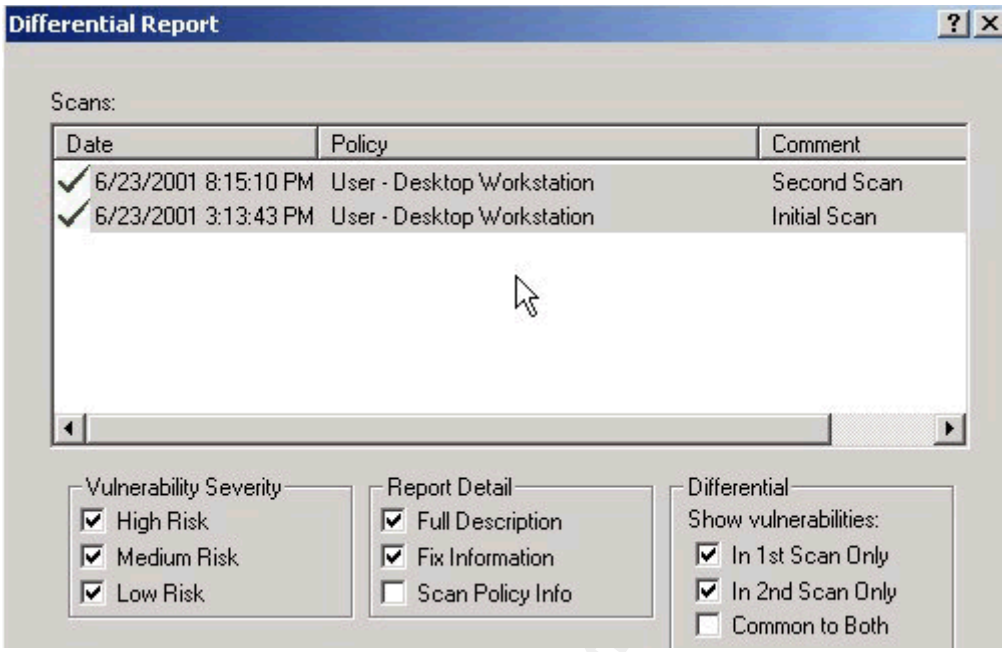


Figure 15 Differential Report Window

16. When viewing the report (See Fig. 16) note that the first scan is the scan with the latest time stamp, and the second scan is the scan with the earliest time stamp. In our example, the first scan is considered the one that has a time stamp of 8:15 PM, and the second scan is the one that has time stamp of 3:13 PM.

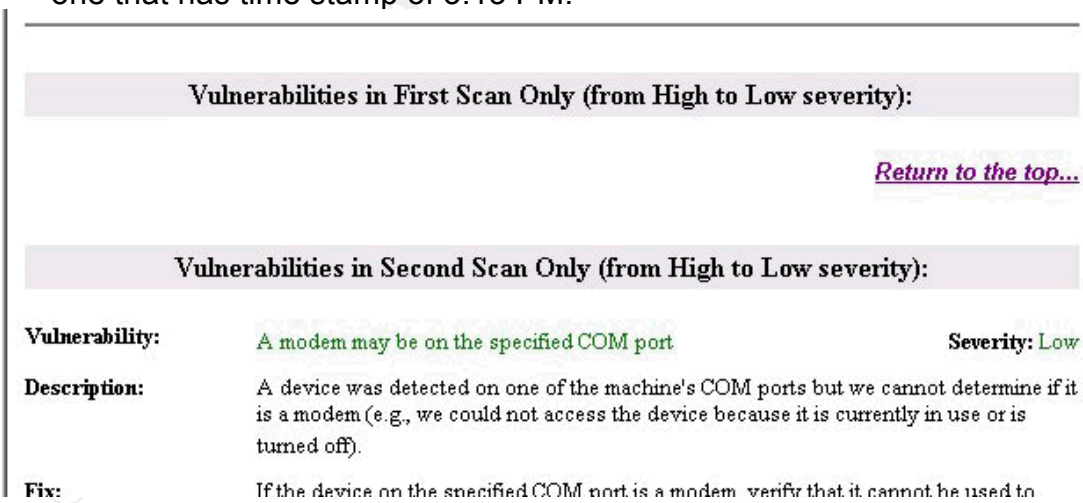


Figure 16 Differential Report Sample

Any vulnerabilities listed under the Vulnerabilities in First Scan Only heading would be new vulnerabilities found since the original scan. We can see that in this case there are none listed.

Any vulnerabilities listed under the Vulnerabilities in Second Scan Only heading are vulnerabilities that have been fixed since the original scan was run. In this case, they could also be vulnerabilities that are no longer being checked for since the original scan but still exist.

© SANS Institute 2000 - 2005 Author retains full rights.

However, once a policy is edited to check for only vulnerabilities that are unacceptable, as done above by deselecting the check for modems, the policy would rarely be modified between scans, so this situation is rare.

Part B - Creating and Scheduling a Policy

This section covers the creation of a new policy, and scheduling that policy to run at certain times. (Recall that System Scanner Agent must be installed as a service to be able to run scans when no one is logged on.) The policy to be created will check the Windows Password Policies, Account Lockout Policies and Auditing Policies for compliance with the settings proposed in "Hardening Windows 2000", (Cox) and in "Windows 2000 Installation Security Checklist" (http://www.labmice.net/articles/securingwin2000.htm, p.3). The settings for the Windows policies are listed below in Table 5.

This System Scanner policy will also attempt to discover users' passwords. There is a dictionary file, nbpw.login, in the installation directory that System Scanner uses to try to guess passwords. Initially it contains a few words, but it is a simple text file, so it can be edited to contain as many words as desirable. This policy will be scheduled to run every Monday and Friday to make sure that no one has changed the Windows policy settings.

System Scanner can also run from the command line, so a report could be scheduled to run from the command line after the scan is completed using Windows built in Task Scheduler. This report could then be mailed or viewed in a web page, so you could check the results of the scan from any computer that has an Internet connection.

Policy	Description	Recommended Setting
Password Policy	Enforce Password History	5
	Maximum Password Age	60
	Minimum Password Age	5
	Minimum Password Length	7
Account Lockout Policy	Account Lockout Duration	30 minutes
	Account Lockout Threshold	5 bad attempts
	Reset Account Lockout Counter After	30 minutes

© SANS Institute 2000 - 2005 Author retains full rights.

Audit Policy	Audit Account Logon Events	Success, Failure
	Audit Account Management	Success, Failure
	Audit Logon Events	Success, Failure
	Audit Object Access	Success
	Audit Policy Change	Success, Failure
	Audit Privilege Use	Success, Failure
	Audit System Events	Success, Failure
	Audit Process Tracking	Disabled

Table 5 Windows Local Security Policy Settings

1. Open up a new policy within System Scanner by clicking on New… in the Policy menu.

2. In the Name of New Policy box, give the policy a descriptive name, in this case Windows Account and Audit Policy Checker.

3. Check the option Let me choose all settings for myself and then click on Next.

4. In the New Policy Wizard window (See Fig. 17), click on the plus sign beside Operating System to expand the tree, then click on the check box beside User checks to activate it and view its' configurable options.

5. Deselect all options except for Audit policies, and Password checks.

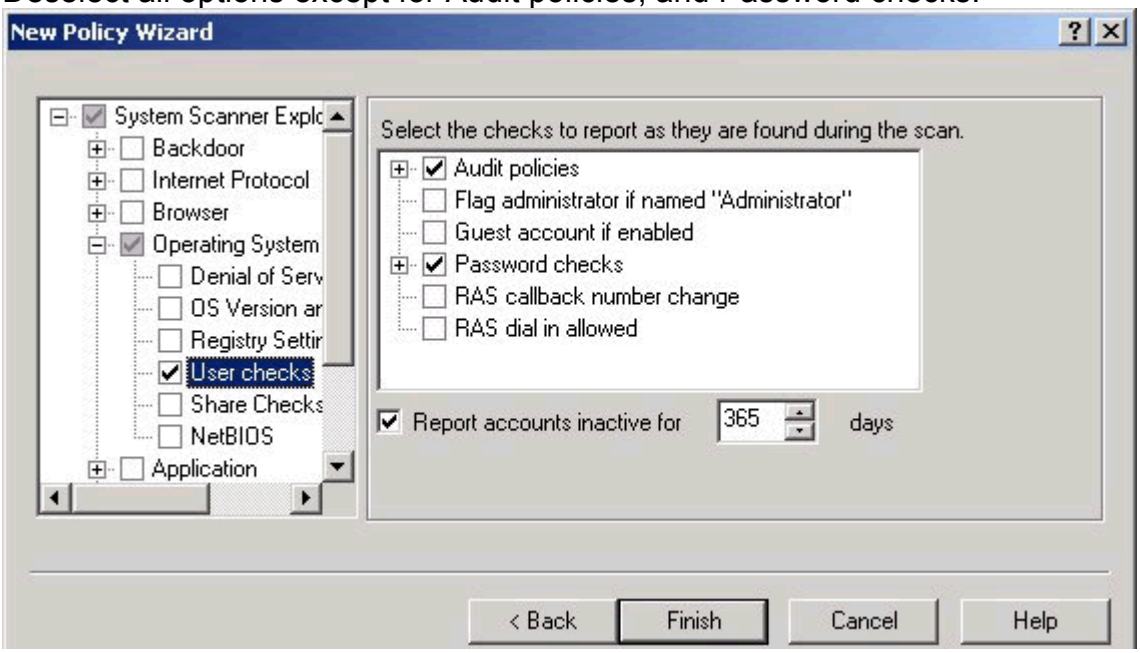


Figure 17 New Policy Wizard

© SANS Institute 2000 - 2005 Author retains full rights.

6. Click on the plus sign beside Audit policies to expand it. There are two subtopics, Success and Failure.

7. Click on the plus sign beside Failure to expand its' options. From the options listed in Table 5 we want to audit failure of all events except for Object Access and Process Tracking. Click the check boxes beside Detailed tracking and Object to deselect them. Note that there is no entry for Account Logon Events. This event type is new to Windows 2000 (Smith), so it was not included in System Scanner 1.1, which was written for NT 4.0.

8. Click on the plus sign beside Success. Here the only option we want to turn off is the Detailed Tracking. Click on the check box beside it to deselect it.

9. Click on the plus sign beside Password checks to view all its options. Deselect all options except for Passwords in dictionary.

10. Scroll down in the left-hand pane to view the Passwords heading. Click the check box beside Passwords to activate it, and then click on the plus sign beside Passwords to see the sub heading Password Settings.

11. Click once on Password Setting to view its' options.

12. In the right hand pane configure all the options according to Table 5. Click on Finish when done to save the policy.

13. Schedule the policy. Choose the Schedule… item from the General menu. This opens the Schedule window where there are currently no scans scheduled.

14. Click on the New… button to schedule a scan. In the Description field (See Fig. 18) enter a description for your scan. From the Policy to use drop down list, choose the newly created scan. For Frequency there is the option of scanning daily, monthly or once only, with all options allowing the time to be specified. For our scan, we will run it on Mondays and Fridays at 6:30 AM.

SANS Institute 2000 - 2005, Author retains full rights.

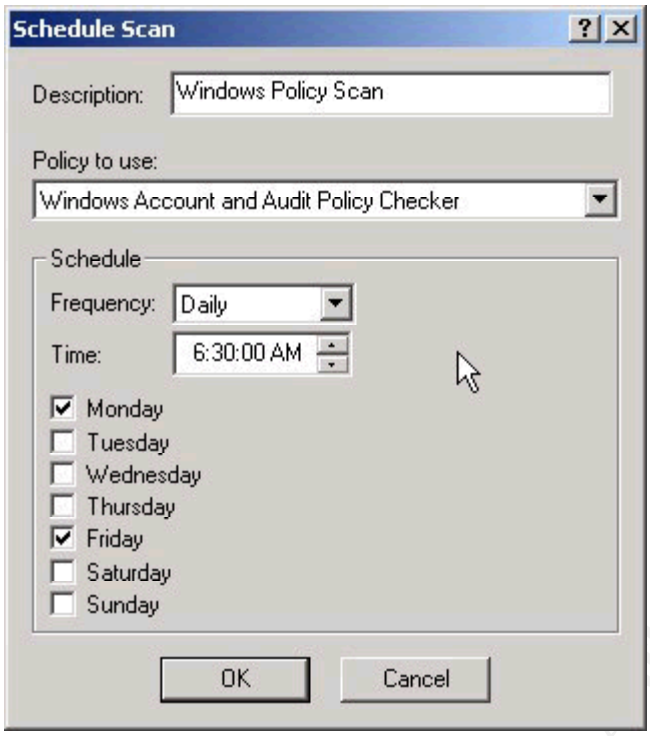


Figure 18 Schedule a Scan

15. Click on OK to save the schedule and view the next scheduled scan in the Schedule Window. (See Fig. 19)

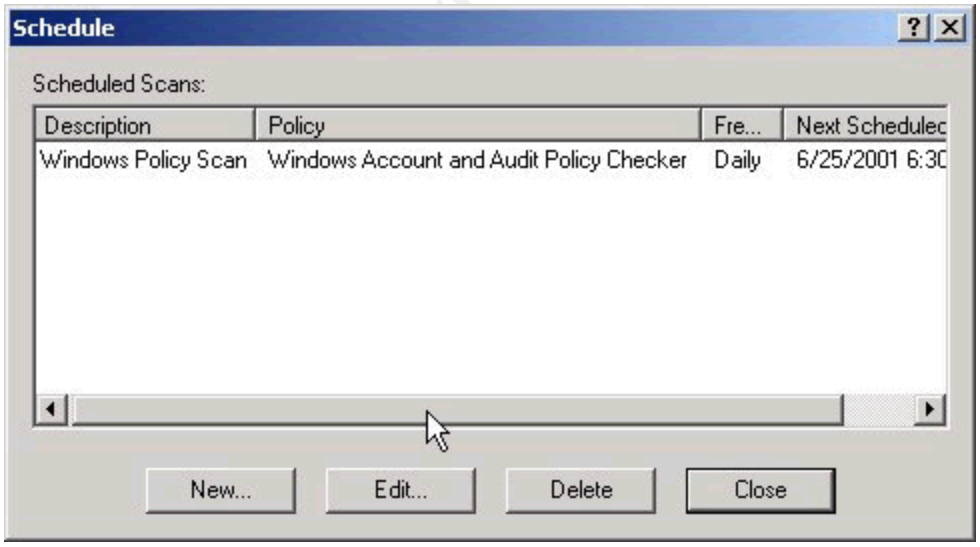


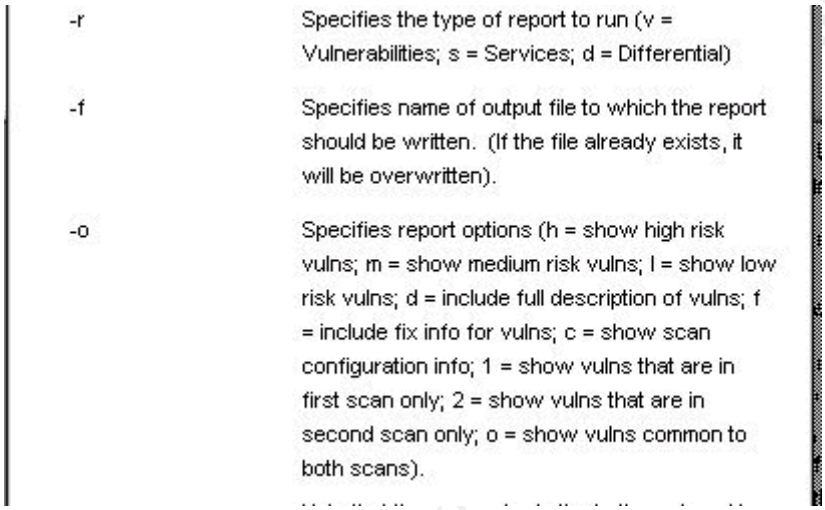
Figure 19 Next Scheduled Scan

16. Before the scheduled scan is run for the first time, remember to change the settings in the Windows Local Security Policy from the defaults to match the settings outlined in Table 5. (Sjouwerman, pp.44, 594) This will ensure that any vulnerabilities found by the scan are the effect of Local Security Policy being changed, not the failure to change the

© SANS Institute 2000 - 2005 Author retains full rights.

settings from their default.

17. System Scanner can be used from the command line to generate reports. To see a list of all command line options, choose the Contents and Index item from the Help menu, double click on How to and double click on Use the Command Line. Click on SSCLI Parameters to get a list of the command line parameters. The options we are concerned with for generating reports are shown below in Figure 20.



-r	Specifies the type of report to run (v = Vulnerabilities; s = Services; d = Differential)
-f	Specifies name of output file to which the report should be written. (If the file already exists, it will be overwritten).
-o	Specifies report options (h = show high risk vulns; m = show medium risk vulns; l = show low risk vulns; d = include full description of vulns; f = include fix info for vulns; c = show scan configuration info; 1 = show vulns that are in first scan only; 2 = show vulns that are in second scan only; o = show vulns common to both scans).

Figure 20 Command Line Options for Reports

18. Create a batch file to run the report. Open a command prompt window. From the command line, type the following (substitute the proper installation path in place of "d:\program files"):
    a. copy con report.bat <enter>
    b. "d:\program files\iss\sysscan\bin\sscli.exe" –r v –f "d:\policy report.html" –o h;m;l;d;f <enter>
    c. <CTRL>Z

    This creates the batch file called "report.bat" that will generate a vulnerability report called "policy report.html", which will include vulnerabilities of all risk levels with full descriptions and fix information. Commands could also be added to the batch file to use a command line e-mail client. After the report is generated it could be mailed, so the report could be viewed from anywhere the administrator has e-mail access.

19. Schedule the batch file to run using Task Scheduler. The full details of using Task Scheduler will not be shown here. (Sjouwerman, p. 504) When scheduling the report to run, be sure to give the scheduled scan enough time to finish. Ten minutes should be more than enough time on most systems, but be sure to pay attention to the scan date on the report when viewing it, to make sure it's not old information. (Note: The second time the batch file runs, the new html report file will overwrite the previous

© SANS Institute 2000 - 2005 Author retains full rights.

one.)

Part C - Monitoring Objects

A very useful part of System Scanner is its' ability to detect changes to your system. It can detect registry and file changes including ownership, permissions, auditing settings and content. It can also detect any changes to a user's account, changes to group membership, user's and group's rights and shared folder changes. (See the full listing in Appendix A, under Exploit Group – Baselines.) It does this by taking a baseline of your system, which can be thought of as a snapshot of the configuration of the objects you want to monitor. The next time a scan runs, if anything has changed from the original snapshot, it is reported.

The policy to be created will monitor a folder and its files for permissions and content changes, monitor the registry's run and runonce keys and the startup folders for changes, and monitor the administrators group for membership changes.

1. Following steps 1 to 3 in Part B, create a new policy called Object Monitor.
2. In the New Policy Wizard window (See Fig. 21), click on the plus sign beside Baselines to view the subheadings.
3. Click on the check box beside Processes to activate it and display its details in the right hand pane. (Since the run registry keys start processes, they are listed under Processes.)
4. Uncheck the Load and Run options, leaving the checking of the registry's run keys and the startup folders enabled.

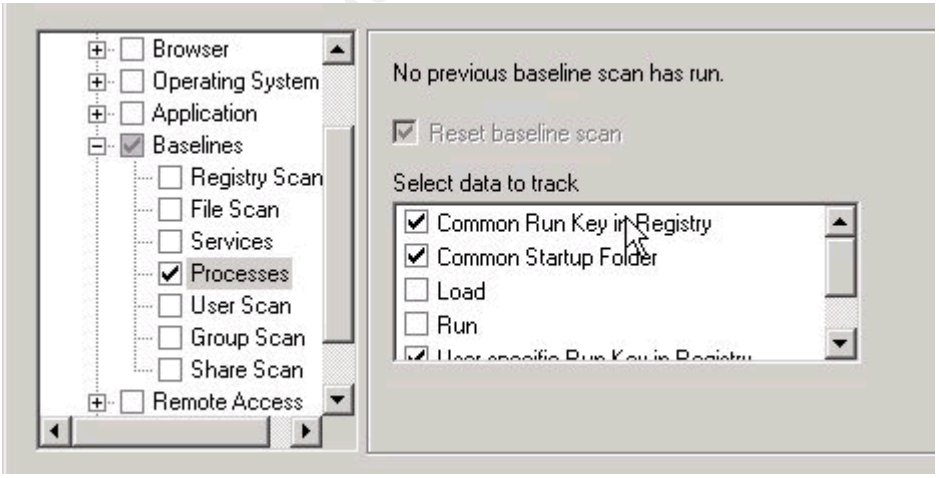


Figure 21 Processes Baselines

5. Click the check box beside File Scan to activate it and display its options in the right hand pane.

© SANS Institute 2000 - 2005 Author retains full rights.

6. On the General tab, under Select Data to Track, check Content and Permissions.

7. Click on the Directories tab and check off the directories that you wish to monitor. In this case d:\documents and settings\administrator\my documents will be monitored.

8. Click on the Extensions tab. (See Fig. 22) Check the list of extensions for the extensions of the files that need to be monitored. If they are not in the list, add them by typing the extension in the box and clicking Add.

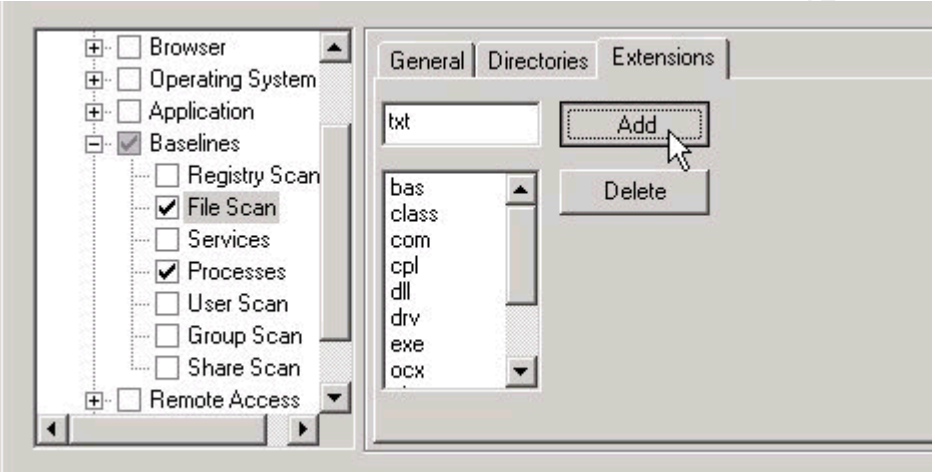


Figure 22 File Scan Baselines

9. Click the check box beside Group Scan to activate it and display its options. We will leave the default of Group Rights and Users in Group activated.

10. Click Finish to save the policy.

11. Run a scan using the new policy. The first time a scan is run with this new policy the baseline is set. (See Fig. 23)

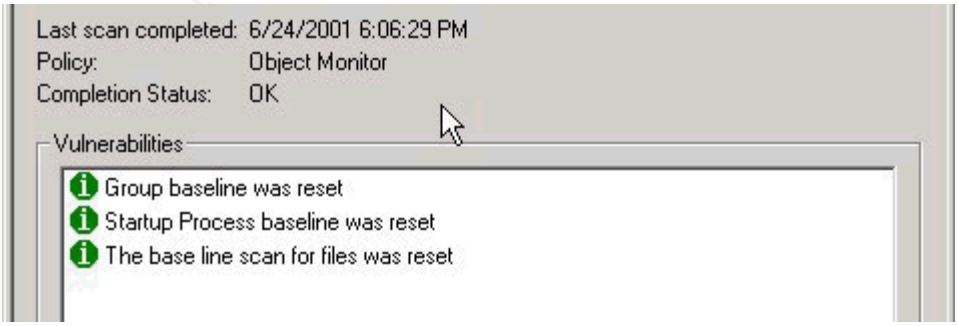


Figure 23 Initial Baseline Set

12. The next scan run with this policy will report any changes made to the

© SANS Institute 2000 - 2005 Author retains full rights.

monitored objects since this baseline. Generate some vulnerabilities by editing one of the files in the monitored directory, adding a user to a group and then rerun the scan. (See Fig 24)

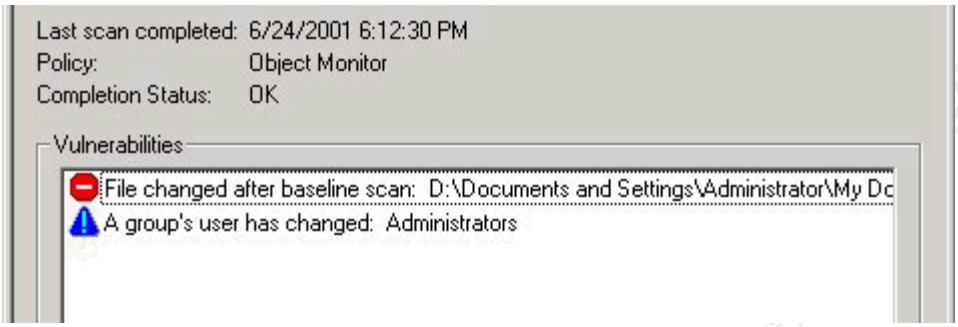


Figure 24 Object Monitor Results

13. After the scan has run, the baselines have to be reset or the same vulnerabilities will be reported the next time a scan is run with that policy. Reset the baselines by choosing the Reset Baselines item from the Policy menu. This opens the Reset Baselines window. (See Fig. 25)

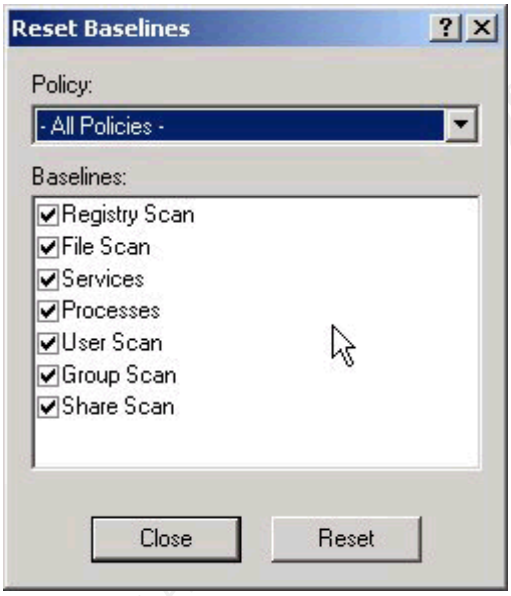


Figure 25 Reset Baselines

14. From the Policy drop down list, choose the Object Monitor policy. Click on Reset, and then click on Close. Doing this tells the Object Monitor policy that the next time a scan is run using the Object Monitor policy, that scan will reset the baselines. A scan with the Object Monitor policy should be run now to avoid missing any changes to the monitored objects.

© SANS Institute 2000 - 2005 Author retains full rights.

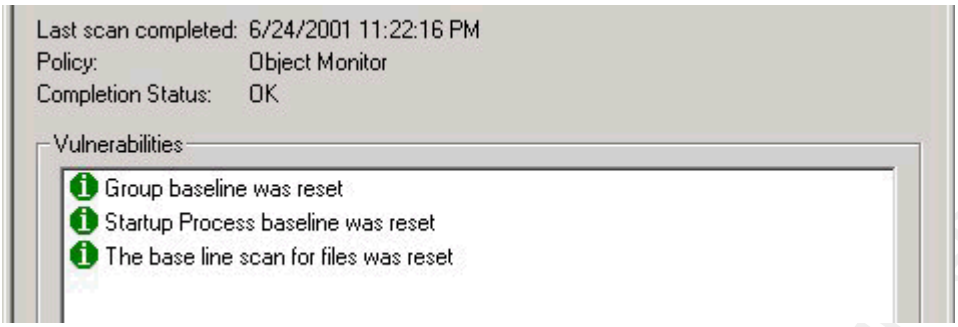


Figure 26 Baselines Now Reset

15. Now the next time a scan is run with the Object Monitor policy, all changes that were made (according to the configuration of the policy) since the baseline was reset will be reported.

Drawbacks/Comprehensiveness

Since System Scanner 1.1 was written for Windows NT, not Windows 2000, it can't be expected to work flawlessly with 2000. A major disadvantage is that there are no longer update files available for System Scanner 1.1, even though the ability to add update files to the software exists. Most, if not all of the IE bug checks, operating system denial of service checks and Office checks are outdated, when run on a system with the latest software. They check for vulnerabilities that have never existed in the latest versions of the software (IE 5, Office 2000, Windows 2000). As well, since there are always new bugs and vulnerabilities being discovered, the lack of updates severely limits System Scanner 1.1's ability as a bug checker.

Additionally, it was noticed a few times that System Scanner gave false results. In Part A of the tutorial, running a predefined policy, it reported that the IIS accounts and the Guest account had blank passwords, even though the IIS accounts had passwords during both scans and the Guest account was given a non blank password after the first scan. In Part B where System Scanner checked the configuration of the Windows Local Security Policy, the scan found the setting for "reset account lockout counter after" to be insufficient, even though the setting in the policy created, and the setting in the Account Lockout policy were the same (30 minutes). The results for that scan also reported some vulnerabilities that the policy wasn't even configured to check for – users that had never logged on and accounts that were set to not expire.

In spite of the aforementioned disadvantages of System Scanner, it does a good job of object monitoring. It is easier and more intuitive to setup a policy to monitor an object in System Scanner, than it is to configure the built-in Windows auditing to monitor the same object. The reports do an excellent job of clearly displaying exactly what object has changed and how, when compared to sifting through the Windows Security Log and trying to interpret the cryptic messages.

However, the information displayed by System Scanner is slightly

© SANS Institute 2000 - 2005 Author retains full rights.

oversimplified. Since the policy is only run at certain times, and not constantly monitoring the system, System Scanner can only tell you if a change was made, not when a change was made or by who. A best practice would be to use a combination of a System Scanner policy to periodically check for changes on objects that require monitoring, as well as using Windows auditing on those objects. When the scan detects a change to one of the objects, the Security log could then be used to pinpoint the exact time the change was made, what was done and by whom.

Comparisons

Cerberus' Internet Scanner

One freeware vulnerability scanner is Cerberus' Internet Scanner. Its' installation is easy (a single executable to run), and updating it is easy. The different vulnerability checks (finger, smtp, NT services, etc.) are kept in separate dll's, so when there is an update to one of them, all that is required is to download the new dll and overwrite the old one. There are currently approximately 250 vulnerability checks available (a full list can be found at http://www.cerberus-infosec.co.uk/vulndb.txt), which is the least amount of checks out of all the products reviewed.

CIS's interface is very simple – a single window, where you can choose the host to scan, what modules to use in the scan, and generate reports. (See Fig. 27) When the scan is running, the progress of each module is listed in the window. However, unlike ISS's System Scanner, when the scan is done, the vulnerabilities found are not displayed in the window. To view the results, a report must be generated.

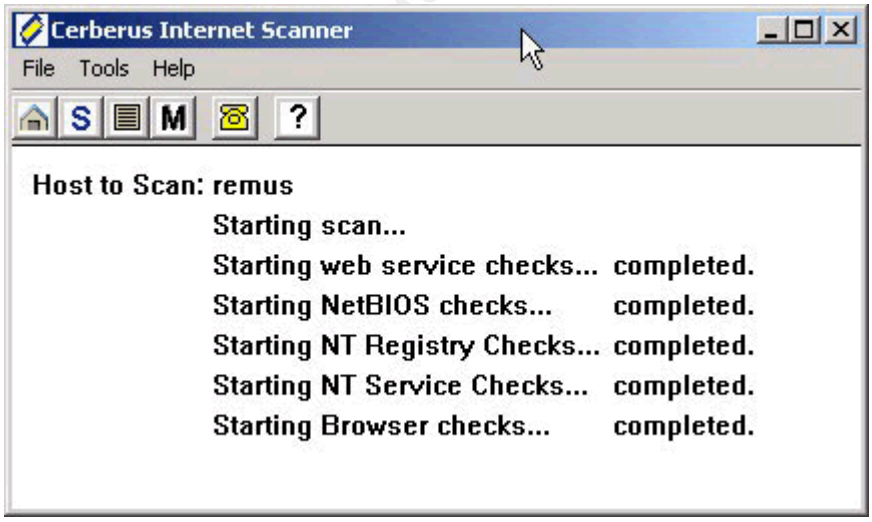


Figure 27 Cerberus Internet Scanner

There is one standard report, which is an html file. The amount of information given on each vulnerability found is okay, but the solutions are

© SANS Institute 2000 - 2005 Author retains full rights.

lacking.

The list of updates for CIS (http://www.cerberus-infosec.co.uk/cis/updates.html) hasn't been updated since May 2000, so there are many new vulnerabilities that won't be detected. This also brings up the question of whether the writing of the product updates has been abandoned.

It's nice to see a freeware scanner for companies with little or no budget for security, but CIS still has a long way to go to catch up to ISS's System Scanner.

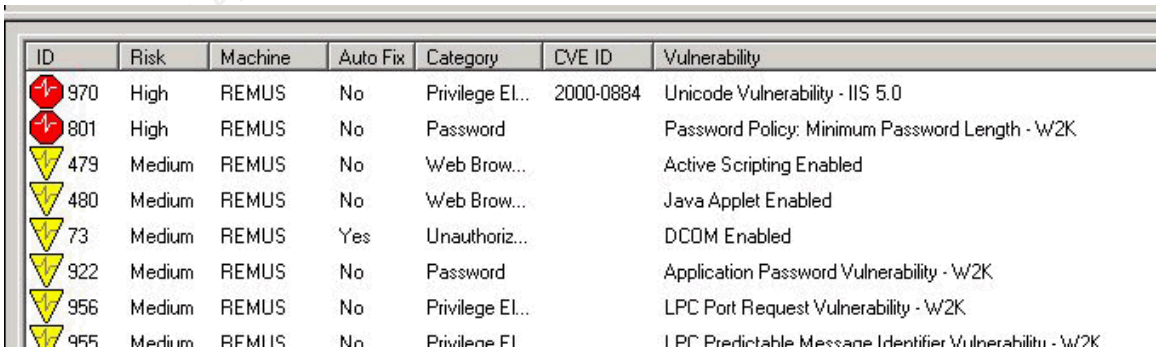
STAT Scanner 4 with Update 1

STAT (Security Threat Avoidance Technology) Scanner is a commercial vulnerability checker. One of the major advantages STAT has over System Scanner version 1.1 is that it is actually written for Windows 2000, as well as NT 4.0, and monthly updates are available for it. As new vulnerabilities are found, STAT can be updated to check for and provide information on them. Currently, there are over 1000 vulnerability checks in STAT Scanner, with approximately 10 to 15 more released with each monthly update, compared to just 272 vulnerability checks for System Scanner 1.1, many of which are nonexistent in a Windows 2000/Office 2000/IE5 configuration.

The basic idea behind STAT Scanner and System Scanner is the same. STAT Scanner uses configuration files to define which vulnerability checks to perform on a computer. An analysis is then run using the configuration file to do the vulnerability checking. After the scan completes, a listing of vulnerabilities is displayed. Information on single vulnerabilities can be viewed by clicking on them, or a report can be generated, which includes detailed information for each vulnerability.

Description of Features

After running an analysis in STAT Scanner, the main window displays the listing of vulnerabilities found, along with their risk, category, CVE-ID number, the vulnerability name and whether an auto fix is available.



ID	Risk	Machine	Auto Fix	Category	CVE ID	Vulnerability
970	High	REMUS	No	Privilege El...	2000-0884	Unicode Vulnerability - IIS 5.0
801	High	REMUS	No	Password		Password Policy: Minimum Password Length - W2K
479	Medium	REMUS	No	Web Brow...		Active Scripting Enabled
480	Medium	REMUS	No	Web Brow...		Java Applet Enabled
73	Medium	REMUS	Yes	Unauthoriz...		DCOM Enabled
922	Medium	REMUS	No	Password		Application Password Vulnerability - W2K
956	Medium	REMUS	No	Privilege El...		LPC Port Request Vulnerability - W2K
955	Medium	REMUS	No	Privilege El...		LPC Predictable Message Identifier Vulnerability - W2K

Figure 28 STAT Analysis Results

© SANS Institute 2000 - 2005 Author retains full rights.

In System Scanner the amount of information included on each vulnerability was good, but with STAT Scanner the amount of information is excellent. Clicking once on a vulnerability to open it, the Description field describes in lengthy detail why the item is considered a vulnerability, and the Solution field gives step by step detailed instructions on how to implement a fix. On the More Info tab there are web links to relevant documents and Microsoft Knowledge Base articles. The Advisories tab has links to articles by advisory boards, such as CERT, on the vulnerability.

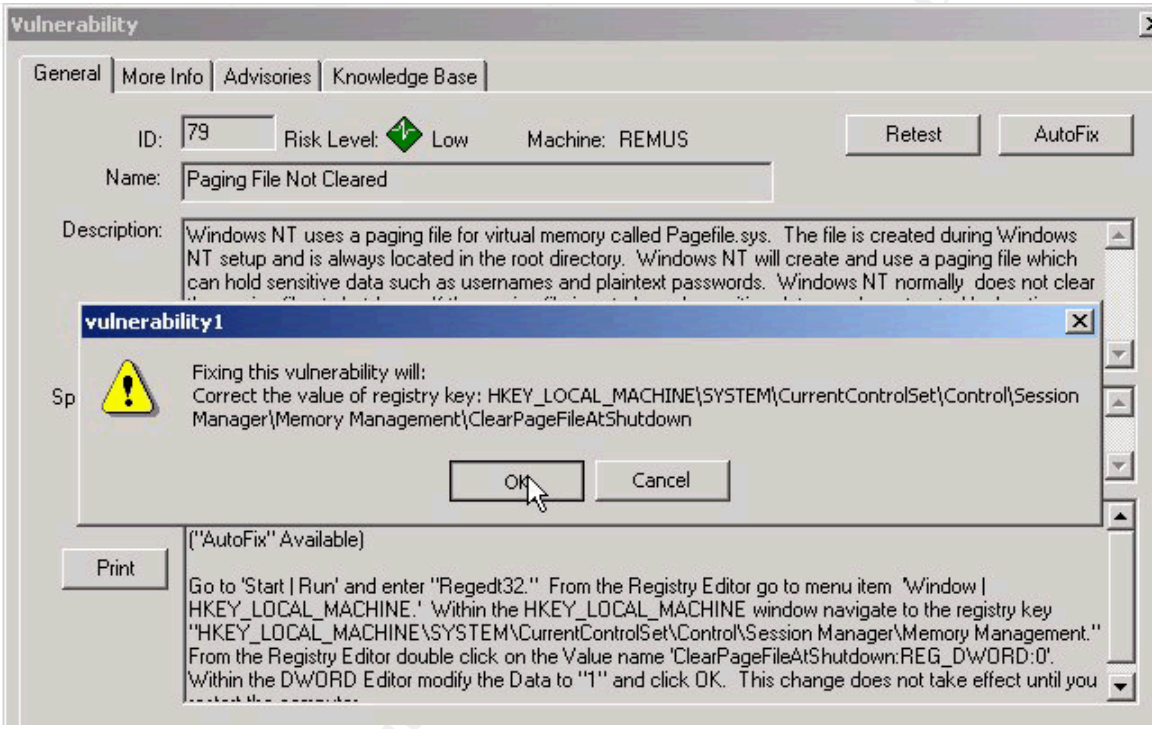


Figure 29 STAT's Auto Fix

STAT Scanner's auto fix feature is very interesting. Opening up a vulnerability that STAT Scanner has listed as being able to Auto Fix, there is an AutoFix button on the General screen, along with a detailed description of the vulnerability, its risk level and a detailed solution. Clicking on the AutoFix button brings up a dialog box (See Fig. 28) stating what STAT Scanner will do to fix the vulnerability, and asks for confirmation. After clicking on OK to confirm that STAT Scanner should fix the vulnerability, STAT Scanner displays a dialog box that the vulnerability has been successfully fixed, and the analysis results window is updated, with the fixed vulnerability no longer being displayed.

This is an excellent time saving feature, especially when there are multiple fixes to be implemented. However, care should be taken when making multiple changes to a system using the Auto Fix feature. It would be a shame to make 25 auto fixes on a system, and then not be able to get into a critical application and have no clue as to which fix broke the application. If this should happen there is an Auto Fix History available by going to the Reports menu, AutoFix History. This will allow you to generate a report listing all the

© SANS Institute 2000 - 2005 Author retains full rights.

vulnerabilities that were automatically fixed after a chosen analysis. This report could then be used to figure out what should be changed back.

If applicable, STAT Scanner also lists the CVE-ID number for the vulnerabilities found. According to Mitre Corporation, CVE "is a list of standardized names for vulnerabilities and other information security exposures – CVE aims to standardize the names of all publicly known vulnerabilities and security exposures" (http://cve.mitre.org/). STAT Scanner is network aware, meaning it has the capability to scan multiple machines. STAT will discover all the machines on a network and filter them according to specified parameters such as operating system and IP subnet. From the list of discovered machines, selections can be made as to which ones should be scanned. Its ability to do this within it's graphical interface is a huge advantage over how System Scanner would be used to scan multiple machines from a central node. The installation of System Scanner would have to be done on all the remote machines, and then command line scans would have to be run on each system.

STAT Scanner's reporting is superior to System Scanner's. There are twelve different reports, as well as a compare scan results option (similar to a Differential Report in System Scanner). The twelve reports cover everything from reports that provide an overview of how many vulnerabilities of each risk level were found, to reports with full details on every vulnerability found.

One area where STAT Scanner doesn't meet or exceed System Scanner is with the ability to schedule a scan on the local system. System Scanner has a GUI scan scheduler for the local system built in, whereas with STAT Scanner you would have to create a batch file to run a scan, and then schedule that batch file with Task Scheduler. STAT Scanner, however, has a built in option to send an e-mail after an analysis has completed, including a copy of the report.

ISS Internet Scanner

ISS's Internet Scanner 6.1 is also a commercial, network enabled system vulnerability scanner and system prober from ISS, the makers of System Scanner. It is similar in functionality to STAT. ISS Internet Scanner has over 700 vulnerability checks built in, and there are installable updates available for it that deal with new vulnerabilities. It is written to run on Windows 2000 Professional or NT 4.0 Workstation. As in System Scanner, policies are created that define what vulnerabilities should be checked for. Then, sessions are created consisting of a policy and a list of hosts to run the policy against. Then a scan can be run using the session.

Description of Features

As with System Scanner once a scan has been run, right clicking on any of the vulnerabilities found opens up window that contains all the information about that vulnerability – risk level, vulnerability name, description of the

© SANS Institute 2000 - 2005 Author retains full rights.

vulnerability, and a solution. ISS Internet Scanner also includes CVE-Ids and it's solutions are more detailed than the solutions offered in System Scanner, but not quite as good as those in STAT Scanner. Appropriate solutions are provided for NT and 2000. Unfortunately, Internet Scanner doesn't have anything that compares to STAT Scanner's AutoFix feature. ISS Internet Scanner has some pretty good features of its own though, including FlexChecks, Smart Scan, and the ability to integrate ISS's Database Scanner and Real Secure Scanner into Internet Scanner.

FlexChecks allow an administrator to create their own vulnerability checks. If there is a new vulnerability that is not checked for in the latest update, then instead of waiting for it to be handled in the next update, an executable could be written in C or Perl to check for the vulnerability. This custom checker can then be added into ISS Internet Scanner by choosing the FlexChecks option from the Tools menu. This brings up the FlexChecks window (See Fig. 29), where you can add in the custom checker by clicking on Add and selecting the executable file. The custom check will then show up in all policies under the FlexChecks heading. Clicking the check box beside the custom check in the policy to be used will run the new check the next time a scan is run.

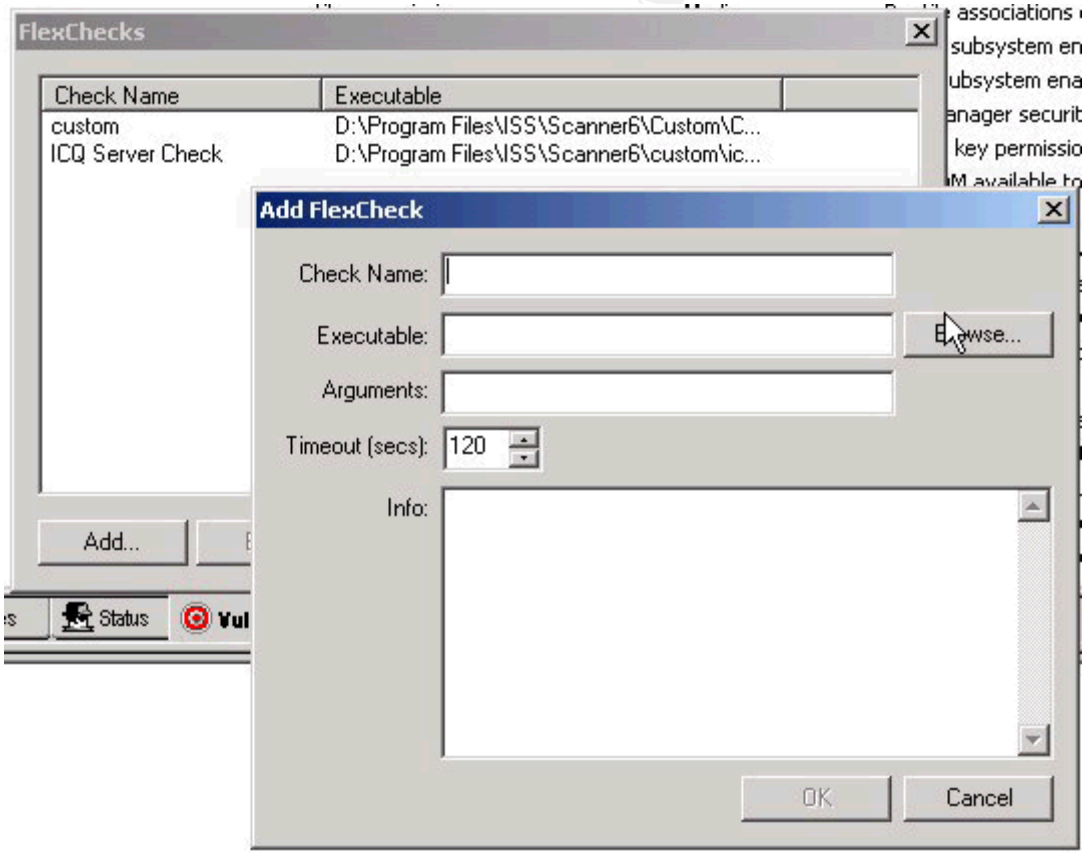


Figure 30 FlexChecks

Integrating Database Scanner into ISS Internet Scanner allows Internet Scanner to run vulnerability checks to find database servers running on the

© SANS Institute 2000 - 2005 Author retains full rights.

network. Internet Scanner can then run vulnerability checks against the databases on those servers to gather information about them and their security. Real Secure is automated real-time intrusion detection and response software. Real Secure uses Internet Scanner to monitor objects and when an attack is detected, Real Secure can respond by disabling the account, or sending a warning message. If implemented properly, this would be an excellent way to maintain system integrity.

With Smart Scan enabled, any account usernames and passwords that are discovered by ISS Internet Scanner are kept in a local file and will be used by later scans to try to discover additional system and network vulnerabilities. Since Internet Scanner can be used for password checking, such as checking for blank passwords, checking for passwords the same as usernames, etc., as well as performing a dictionary attack to try to determine passwords, chances are that it will be able to compromise at least a few accounts on any network. These accounts are then kept in a file, whose location can be set by going to Tools – Options and clicking on the File Locations tab and looking in the KnownAccounts file location box. (See Fig. 30) Note that the dictionary file location and pwd directory can also be set here.

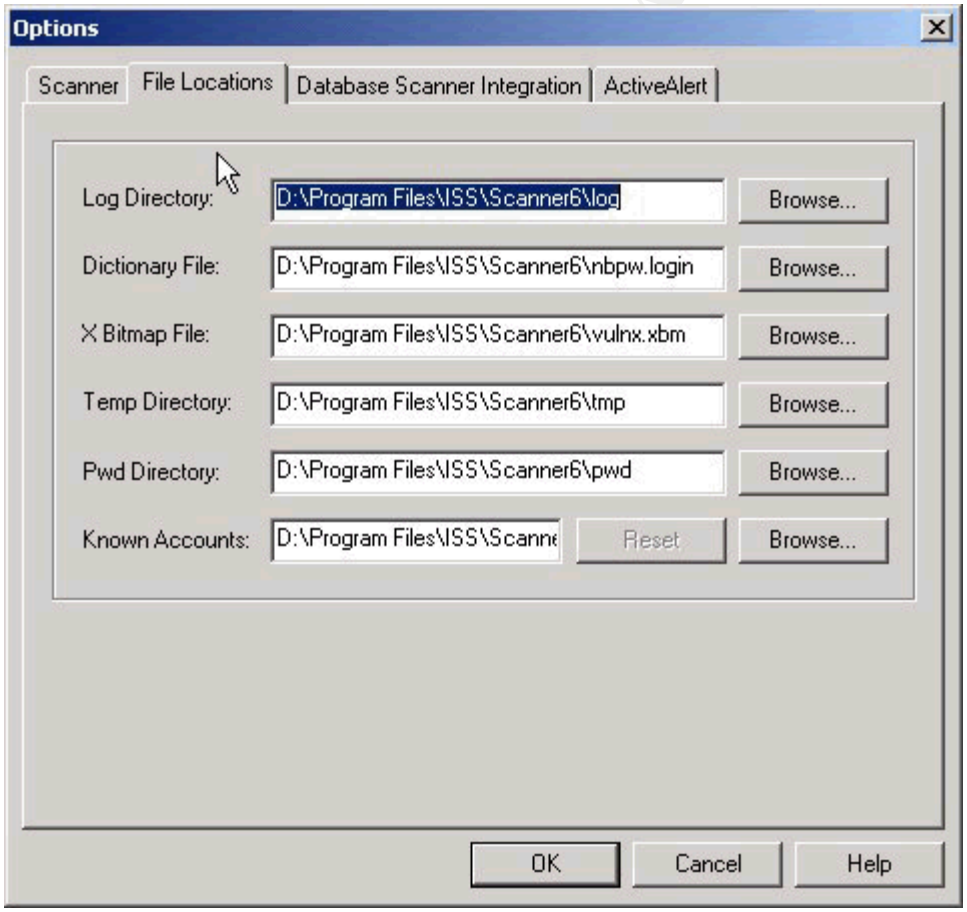


Figure 31 File Locations

The pwd directory is the repository for any sensitive files ISS Internet

© SANS Institute 2000 - 2005 Author retains full rights.

Scanner finds when scanning system, such as pwl files, if ISS Internet Scanner is set to grab these files (set under Tools – Options – Scanner tab, Grab Critical Files).

Also on the Tools menu is the Edit Known Accounts item. Clicking on this brings up a window that contains the known accounts and their passwords. Accounts can also be added to this list, if a username and password are known or suspected. If the password is known, then the account can be configured as verified. This means that ISS Internet Scanner will use it to attempt to establish logon sessions with the target computers using this account even if there are account lockout policies in place. If the account is configured as not verified, then ISS Internet Scanner will attempt to use the account to establish logon sessions only if there is no account lockout policy in place on the target.

The reports that ISS Internet Scanner can generate are on the same level as those generated by STAT Scanner. There are over 30 built in reports that range from pie graphs showing the number of vulnerabilities in each risk level shown, to reports that list each vulnerability with descriptions and solutions included. There is also the ability to import custom reports that can be created with Crystal Reports.

A comparison of features of all scanners reviewed is shown in Table 6.

Product	No. of Vulnerabilities	Amount of Info	Auto Fix	CVE Compatible	GUI Scheduler	Command Line Operation	No of Reports
ISS System Scanner	~270	Decent	No	No	Yes	Yes	4
Cerberus Internet Scanner	~250	Sparse	No	No	No	No	1
STAT Scanner	1000+	Excellent	Yes	Yes	No	Yes	12
ISS Internet Scanner	700+	Excellent	No	Yes	Yes	Yes	30, plus custom reports

Table 6 Comparison of Features

Conclusions

As a tool included with the Windows 2000 Server Resource Kit, System Scanner could prove to be valuable for easily monitoring objects for changes, and quickly checking Windows Local Security Policy settings for compliance with a company standard. The information it includes in reports is decent, making it fairly easy to correct the vulnerabilities it finds. However, since new exploits are being found all the time, its lack of updates makes it unreliable as an exploit checker, and some of the false results it generates could make it difficult to deal with.

The freeware Cerberus Internet Scanner has the same major downside to it that System Scanner does – lack of checking for new, current vulnerabilities.

© SANS Institute 2000 - 2005 Author retains full rights.

The vulnerability descriptions and solutions are the least informative of all the products reviewed. Using this product could give an unaware administrator a false sense of security.

STAT Scanner and ISS Internet Scanner both look to be excellent commercial system scanners. They both check for far more vulnerabilities than ISS System Scanner and CIS. STAT Scanner's ability to automatically fix vulnerabilities, and the amount of information it includes in descriptions and proposed solutions make it an attractive product. However, ISS Internet Scanner's ability to incorporate custom checks into it's scans, and it's ability to integrate with Database Scanner and Real Secure give it increased functionality that doesn't exist in STAT.

If one of the commercial tools is not in the budget, and object monitoring or policy settings checking is the primary concern, then System Scanner is a decent product. But if the security of all systems on the network is of utmost importance, then one of the commercial products would be the best choice.

© SANS Institute 2000 - 2005, Author retains full rights.

Appendix A – System Scanner 1.1's Full Vulnerability Listing

Exploit Group	Exploit	Vulnerability Name	Vulnerability ID	OS Affected
Backdoor (1)	NetBus (1)	NetBus Installed	win-netbus-installed	Windows 95,Windows 98,Windows NT
Internet Protocol (5)	Service Scan (1)	Finger Service	finger-running	finger svc
	FTP (4)	Files obtained	filesgrabbed	Any
		Anonymous FTP enabled	ftp-anon	Any
		FTP site exec vulnerable	ftp-exec	wu-ftpd:2.4.1 and earlier.
		Writeable ftp directories	ftp-write	Any
Browser (26)	Internet Explorer (19)	IE Embed bug	ie-embed	Windows 95,Windows NT
		IE mk bug	iemk-bug	Windows 95,Windows NT
		Internet Explorer vulnerability	ie-ver	Windows 95,Windows NT
		The Java Script patch is not applied	java-script-patch	Windows 95,Windows 98,Windows NT
		URL Security Zone scripting safe Active X controls.	zone-safe-scripting	Windows 95,Windows NT
		URL Security Zone Signed Active X download	zone-signed-download	Windows 95,Windows NT
		URL Security Zone Unsigned Active X download.	zone-unsigned-download	HPUX,Windows 95,Windows NT
		URL Security Zone scripting of unsafe Active X controls.	zone-unsafe-scripting	Windows 95,Windows NT
		URL Security Zone Active X execution	zone-activeX-execution	Windows 95,Windows NT
		URL Security Zone scripting safe Active X controls.	zone-safe-scripting	Windows 95,Windows NT
		URL Security Zone Auto user authentication	zone-auto-authenticate	Windows 95,Windows NT
		URL Security Zone file download	zone-file-download	Windows 95,Windows NT
		URL Security Zone low java permissions	zone-low-java	Windows 95,Windows NT
		URL Security Zone low channel permissions	zone-low-channel	Windows 95,Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

		URL Security Zone file launch	zone-file-launch	Windows 95,Windows NT
		URL Security Zone desktop install	zone-desktop-install	Windows 95,Windows NT
		URL Security Zone non-secure form submission	zone-form-submission	Windows 95,Windows NT
		URL Security Zone java scripting	zone-java-scripting	Windows 95,Windows NT
		URL Security Zone active scripting	zone-active-scripting	Windows 95,Windows NT
	Netscape Navigator (7)	Netscape Navigator is outdated	nav-outdated	Windows 95,Windows NT:4.0
		Netscape Navigator entering a secure site warning is disabled.	nav-enter-secure-site	Windows 95,Windows NT:4.0
		Netscape Navigator non-secure form submission warning is disabled.	nav-non-secure-submission	Windows 95,Windows NT:4.0
		Netscape Navigator has JavaScript enabled.	nav-javascript-enabled	Windows 95,Windows NT:4.0
		Netscape Navigator leaving a secure site warning is disabled.	nav-leave-secure-site	Windows 95,Windows NT:4.0
		Netscape Navigator mixed document security warning is disabled.	nav-mixed-doc	Windows 95,Windows NT:4.0
		Netscape Navigator has Java Enabled.	nav-java-enabled	Windows 95,Windows NT:4.0
Operating System (113)	Denial of Service (17)	IIS ASP Dot Bug	http-iis-aspsource	Windows NT
		Chargen Patch not Applied	chargen-patch	Windows NT
		DNS Predictable Query	dns-predict-query	Windows NT
		DNS Version Denial Of Service	nt-dnsver	Windows NT
		Getadmin Patch not applied	nt-getadmin	Windows NT
		IIS CGI Overflow	http-iis-cgi	Windows NT
		Windows NT Kernel Outdated	nt-kernvers	Windows NT
		Land denial of service attack	land	Any
		Lan Manager Security	lanman-sec	Windows 95,Windows NT
		Out of band DoS	win-oob	Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

		Missing PowerPoint Security Patch	nt-ppt-patch	Windows NT
		Unauthorized user can debug programs.	nt-priv-patch	Windows NT
		Outdated RPC Locator Service	nt-rpc-ver	Windows NT
		Missing Post-SP2 Security Patches	nt-sp2	Windows NT
		Ssping Patch not Applied	nt-ssping	Windows NT
		missing syncstorm patch	nt-syncstormpatch	Windows NT
		WINS Patch not Applied	nt-wins-patch	Windows NT
	OS Version and Service Packs (1)	Update to OS is available.	os-update-avail	Windows 95,Windows NT
	Registry Settings (29)	Autologon Is Enabled	nt-autologon	Windows NT
		Autologon Password Readable	nt-autologonpwd	Windows NT
		Page File not Cleared at Shutdown	nt-clearpage	Windows NT
		DCOM is Enabled.	nt-dcom	Windows NT
		DCOM Can Be Enabled By Non-Admins	nt-dcomperms	Windows NT
		DCOM RunAs Value Altered	nt-dcom-runas	Windows NT
		DCOM RunAs Value Writeable	nt-dcom-runaswrite	Windows NT
		GetAdmin Present on Host	nt-getadmin-present	Windows NT
		IP Forwarding Enabled	ip-forwarding	Windows NT
		Lan Manager Security	lanman-sec	Windows 95,Windows NT
		Multihomed Host	nt-multihomed	Windows NT
		Multiple Protocols Active	nt-multiprotocol	Windows NT
		AutoRun setting not default	nt-autorun-notdefault	Windows 95,Windows NT
		OS/2 Subsystem Enabled	nt-os2-sub	Windows NT
		Performance Monitor Readable	nt-perfmon	Windows NT
		Posix Enabled	nt-posix	Windows NT
		AutoRun is set for RAM disks	nt-ramdisk-autorun	Windows 95,Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

		Windows NT Remote Access service running	nt-ras	Windows NT
		Regedit Is Associated With .reg Files	nt-regfile	Windows NT
		Regfile Associations Can Be Changed By Non-Admins	nt-regfileperm	Windows NT
		Scheduler Key Has Incorrect Permissions	nt-schedule-perm	Windows NT
		SNMP Community Name Is World Readable By Default	nt-snmp	Windows NT
		NetBIOS Information Available From SNMP	snmp-netbios	Windows NT
		Windows Key with Incorrect Permissions	nt-keyperm	Windows NT
		Winlogon Key Has Incorrect Permissions	nt-winlogon-perm	Windows NT
		Registry Access Unrestricted From Network	nt-winreg-net	Windows NT
		Registry Access Allowed For All Users	nt-winreg-all	Windows NT
		HKEY_CLASSES Writeable By Everyone	nt-hkey-classeswrite	Windows NT
		HKEY_LOCAL Writeable By Non-Administrators	nt-hkey-local	Windows NT
	User checks (46)	User Account Has Blank Password	nt-accountblankpw	Windows NT
		User Account Has a Password the Same as the Account Name	nt-accountuserpw	Windows NT
		NT Administrator Has Blank Password	nt-adminblankpw	Windows NT
		Default NT Administrator Userid Exists	nt-adminexists	Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

Administrator Account Has Password The Same As The Account Name	nt-adminuserpw	Windows NT
Guessed Windows NT Administrator Password	nt-guess-admin	Windows NT
Guessed Windows NT Guest Password	nt-guess-guest	Windows NT
Guessed Windows NT Account Password	nt-guess-user	Windows NT
NT Guest User Has Blank Password	nt-guestblankpw	Windows NT
NT Guest Account Enabled	nt-guest	Windows NT
Guest Account Has a Password the Same as the Account Name	nt-guestuserpw	Windows NT
A new user was added	nt-newuser	Windows NT
A user has can change callback number	nt-user-changedialin	Windows NT
A user has Dialin permission	nt-user-dialin	Windows NT
A user account is dormant	nt-user-dormant	Windows NT
User never logged on	nt-user-neverloggedon	Windows NT
A user has no password	nt-nopw	Windows NT
A user's password never expires	nt-user-pwnoexpire	Windows NT
Inappropriate User with Act as System Privilege	nt-act-system	Windows NT
Inappropriate User with Add Workstation Privilege	nt-add-workstation	Windows NT
System Auditing not Enabled	nt-system-audit	Windows NT
Logon Auditing not Enabled	nt-logon-audit	Windows NT
Object Auditing not Enabled	nt-object-audit	Windows NT
Privilege Auditing not Enabled	nt-privil-audit	Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

Process Auditing not Enabled	nt-process-audit	Windows NT
Policy Auditing not Enabled	nt-policy-audit	Windows NT
Account Management Auditing not Enabled	nt-account-audit	Windows NT
Inappropriate User with Backup Privilege	nt-backup	Windows NT
Inappropriate User with Change System Time Privilege	nt-system-time	Windows NT
Inappropriate User with Create Pagefile Privilege	nt-create-pagefile	Windows NT
Inappropriate User with Create Permanent Object Privilege	nt-create-object	Windows NT
Inappropriate User with Create Token Name Privilege	nt-create-token	Windows NT
Inappropriate User with Debug Privilege	nt-debug	Windows NT
Inappropriate User with Generate Security Audit Privilege	nt-sec-audit	Windows NT
Inappropriate User with Increase Priority Privilege	nt-increase-priority	Windows NT
Inappropriate User with Increase Quota Privilege	nt-increase-quota	Windows NT
Inappropriate User with Load Driver Privilege	nt-load-driver	Windows NT
Inappropriate User with Lock Memory Privilege	nt-lock-memory	Windows NT
Inappropriate User with Profile Single Process Privilege	nt-single-process	Windows NT
Inappropriate User with Profile System Privilege	nt-profile-system	Windows NT
Inappropriate User with Remote Shutdown Privilege	nt-remote-shutdown	Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

		Inappropriate User with Replace Process Token Privilege	nt-replace-token	Windows NT
		Inappropriate User with Restore Privilege	nt-restore	Windows NT
		Inappropriate User with System Environment Privilege	nt-system-env	Windows NT
		Inappropriate User with Take Ownership Privilege	nt-take-owner	Windows NT
		Inappropriate User with Unsolicited Input Privilege	nt-unsol-input	Windows NT
	Share Checks (8)	NetBIOS share found	nt-netbios-share	OS/2,Unix samba,Windows 95,Windows for Workgrou:3.11,Windows NT
		Insecure File System	nt-filesys	OS/2,Windows 95,Windows for Workgrou:3.11,Windows NT
		The NTFS directory being shared is not secure	nt-insecure-ntfs	Windows NT
		NetBIOS Share Has No Access Control	nt-netbios-open	Windows NT
		All Access NetBIOS Share - Everyone	nt-netbios-everyoneaccess	Windows NT
		All Access NetBIOS share - Guest	nt-netbios-guestaccess	Windows NT
		Writeable NetBIOS Share - Everyone	nt-netbios-write	Windows NT
		Writable NetBIOS share - Guest	nt-netbios-shareguest	Windows NT
	NetBIOS (12)	Repair Directory Readable	nt-repair	Windows NT
		Alerter and messenger services	nt-alerter	Windows NT
		Windows NT Messenger service running	nt-messenger	Windows NT
		NT Network Monitor	nt-netmon	Windows NT
		NT Rlogin Service Installed	nt-rlogin	Windows NT
		Insecure File System	nt-filesys	OS/2,Windows 95,Windows for Workgrou:3.11,Windows NT
		Windows NT rcmd service running	nt-rcmd	Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

		Windows NT Rexec Service Running	rexec	Any
		Windows NT Rsh Service Running	rsh-svc	Windows NT
		Windows NT Schedule Service Running	nt-schedule	Windows NT
		NT Telnet Service Installed	nt-telnet	Windows NT
		Unknown NT Service	nt-unknown-svc	Windows NT
Application (39)	MS Office (3)	One or more Office 97 files are out of date.	office97-internet	Windows 95,Windows NT
		PowerPoint Viewer	ppt-view	Windows 95,Windows NT
		Outlook long file name patch not applied	outlook-long-name	Windows 95,Windows NT
	Virus Scanner (1)	No Anti-virus Software Installed.	no-antivirus-installed	Windows 95,Windows NT
	PWS (35)	8.3 File Names Enabled on Web Server	iis-check-8.3-registry	Windows NT
		Indexed Directory with .asp files	iis-check-indexed	Windows NT
		Basic HTTP Authentication Enabled	iis-basic-http-auth	Windows NT
		Browsing Enabled for Web Directory	iis-check-dir-browse	Windows NT
		Client Script Debugging Enabled	iis-check-client-debug	Windows NT
		IIS CGI scripts run as system	iis-create-process	Windows 95,Windows NT
		Unauthorized user can access IIS files	iis-data-patch	IIS:3.0 and earlier,Windows NT
		Developer Tools on Web Server	iis-check-dev-tools	Windows NT
		Incoming FTP executable check	iis-check-ftp-dacl	Windows NT
		Insecure Web Password Change Enabled	iis-auth-change	Windows NT
		Non-anonymous FTP Login Enabled	non-anonymous	Windows NT
		Web directory with no security check	iis-check-web	Windows NT
		Restricted Web directory with no security	iis-check-restricted	Windows NT
		FTP directory check	iis-check-ftp-dir	Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

		Microsoft Office Installed on Web Server	iis-check-msoffice	Windows NT
		Parent Paths Enabled for .asp pages	iis-check-parent-paths	Windows NT
		IIS Passive FTP patch not applied	iis-passive-ftp	IIS:3.0 and earlier,Windows NT
		Web Directories With Crossing Paths	iis-check-crossing-paths	Windows NT
		IIS incorrect web permissions	iis-perm	Windows NT
		IIS incorrect permissions on restricted item	iis-perm-restr	Windows NT
		Port Attack Enabled on FTP Server	iis-check-enable-port-attack	Solaris:2.x,SunOS:4.1.x,Windows NT
		IIS Unauthorized ODBC Data Access with RDS and IIS	nt-iis-rds	Windows 95:with default setting,Windows NT
		IIS Samples Installed on Web Server	iis-check-samples	Windows NT
		IIS Server Script Debugging Enabled	iis-check-server-debug	Windows NT
		IWAM User in Incorrect Group	iis-check-iwam-groups	Windows NT
		IIS Special characters allowed in shell	iis-special-chars	Windows 95,Windows NT
		IIS SSL patch not applied	iis-ssl-patch	IIS:3.0 and earlier,Windows NT
		IUSR User in Incorrect Group	iis-check-iusr-groups	Windows NT
		IWAM User in Incorrect Group	iis-check-iwam-groups	Windows NT
		IIS Version 2 installed	iis-v2	Windows 95,Windows NT
		Executable Web Directory Check.	iis-check-executable-webdir	Windows NT
		Writable FTP Directory can be read	iis-check-ftp-writable	Windows NT
		Writable Web Directory check	iis-check-writable-webdir	Windows NT
		Wscript Present on Web Server	iis-check-script	Windows 95,Windows NT
		Cscript Present on Web Server	iis-check-script-engines	Windows 95,Windows NT
Baselines (69)	Registry Scan (9)	New registry key found	reg-key-added	Windows 95,Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

	The security permissions for a registry key have changed	nt-regkeychanged-dacl	Windows NT
	The owner of a registry key has changed	nt-regkeychanged-owner	Windows NT
	The audit settings of a key have changed	nt-regkeychanged-sacl	Windows NT
	Registry key missing	reg-key-deleted	Windows 95,Windows NT
	New registry value found	reg-value-added	Windows 95,Windows NT
	Registry value changed	reg-value-changed	Windows 95,Windows NT
	Registry value missing	reg-value-deleted	Windows 95,Windows NT
	Registry baseline was reset	nt-reset-registry-baseline	Windows 95,Windows NT
File Scan (14)	The attributes for a folder have changed	nt-changedscandir-attrib	Windows NT
	The security permissions for a folder have changed	nt-changedscandir-dacl	Windows NT
	The owner of a folder has changed	nt-changedscandir-owner	Windows NT
	The audit settings of a folder have changed	nt-changedscandir-sacl	Windows NT
	File changed after baseline scan	nt-changedscanfile	Windows 95,Windows NT
	The attributes for a file have changed	nt-changedscanfile-attrib	Windows NT
	The security permissions for a file have changed	nt-changedscanfile-dacl	Windows NT
	The owner of a file has changed	nt-changedscanfile-owner	Windows NT
	The audit settings of a file have changed	nt-changedscanfile-sacl	Windows NT
	A folder was deleted after baseline scan	nt-dir-deleted	Windows 95,Windows NT
	A file was deleted after baseline scan	nt-file-deleted	Windows 95,Windows NT
	New folder after baseline	nt-newscan-dir	Windows NT
	New file after baseline	newscan-file	Windows 95,Windows NT
	The base line scan for files was reset	reset-file	Windows 95,Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

Services (18)	Service's Binary Path Name has changed	nt-changedservice-binary	Windows NT
	Control codes the service will accept/process have changed	nt-changedservice-controls	Windows NT
	A service's current state has changed	nt-changedservice-current	Windows NT
	Service's Discretionary Access-Control List has changed	nt-changedservice-dacl	Windows NT
	A service's Display Name has changed	nt-changedservice-display	Windows NT
	Service Error Control has changed	nt-changedservice-error	Windows NT
	Service's Load Order Group has changed	nt-changedservice-load	Windows NT
	Service's Owner has changed	nt-changedservice-owner	Windows NT
	Service's System Access-Control List has changed	nt-changedservice-sacl	Windows NT
	Service's Start Name has changed	nt-changedservice-startname	Windows NT
	Service Start Type has changed	nt-changedservice-startup	Windows NT
	Service's Tag ID has changed	nt-changedservice-tag	Windows NT
	A service's type has changed	nt-changedservice-type	Windows NT
	Service Wait Hint interval has changed	nt-changedservice-wait	Windows NT
	A new service was added	nt-service-added	Windows NT
	Service baseline was reset	nt-resetservice-baseline	Windows NT
	A service was deleted	nt-service-deleted	Windows NT
	Max vulns logged for this exploit	exploit-limit	Windows 95,Windows NT
Processes (5)	A Startup Process has changed	nt-changed-startup	Windows NT
	A new startup process was added	nt-new-startup	Windows NT
	Startup Process baseline was reset	nt-reset-process	Windows NT
	A startup process was deleted	nt-startup-process	Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

		Max vulns logged for this exploit	exploit-limit	Windows 95,Windows NT
	User Scan (7)	A user's group membership has changed	nt-changeduser-groups	Windows NT
		A user's logon information has changed	nt-changeduser-logoninfo	Windows NT
		A user's rights have changed	nt-changeduser-privs	Windows NT
		A user's Dialin settings have changed	nt-changeduser-ras	Windows NT
		Max vulns logged for this exploit	exploit-limit	Windows 95,Windows NT
		A user was deleted	nt-user-deleted	Windows NT
		User baseline was reset	nt-resetuser-baseline	Windows NT
	Group Scan (6)	A group's rights have changed	nt-changedgroup-privs	Windows NT
		A group's user has changed	nt-changedgroup-users	Windows NT
		A Group was deleted	nt-group-deleted	Windows NT
		A new Group was added	nt-new-group	Windows NT
		Group baseline was reset	nt-resetgroup-baseline	Windows NT
		Max vulns logged for this exploit	exploit-limit	Windows 95,Windows NT
	Share Scan (10)	An NTFS share's permissions have changed	nt-changed-ntfs-dacl	Windows NT
		An NTFS share's audit settings have changed	nt-changed-ntfs-sacl	Windows NT
		An NTFS share's owner has changed	nt-changed-ntfs-owner	Windows NT
		A share's permissions have changed	nt-changed-dacl	Windows NT
		A share's audit settings have changed	nt-changed-sacl	Windows NT
		A share's owner has changed	nt-changed-owner	Windows NT
		A new share was added	nt-new-share	Windows NT
		Share baseline was reset	nt-reset-share	Windows NT
		A share was deleted	nt-share-deleted	Windows NT
		Max vulns logged for this exploit	exploit-limit	Windows 95,Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

Remote Access (10)	Modems (4)	A modem was found	nt-found-modem	Windows NT
		A modem configured for AutoAnswer was found	nt-modem-autoanswer	Windows 95,Windows NT
		A modem configured for AutoAnswer was found and Dial Tone was detected on the phone line	nt-modem-dialtone	Windows 95,Windows NT
		A modem may be on the specified COM port	nt-possible-modem	Windows NT
	pcANYWHERE32 (1)	pcANYWHERE32 is installed	pcanywhere32-installed	Windows 95,Windows NT
	Carbon Copy 32 (1)	Carbon Copy 32 is installed	carboncopy32-installed	Windows 95,Windows NT
	Remotely Possible/32 (1)	Remotely Possible/32 is installed	remotelypossible32-installed	Windows 95,Windows NT
	LapLink (2)	LapLink is installed	laplink-installed	Windows 95,Windows NT
		Remote DeskLink for Windows 95 is installed	remote-desklink-installed	Windows 95
	RAS (1)	Found a RAS port configured to receive calls	nt-ras-dialin	Windows NT
Passwords (9)	Password Settings (9)	Forced Logoff Not Enabled	nt-force-logoff	Windows NT
		Lockout Threshold Incorrect	nt-thres-lockout	Windows NT
		Password lockout disabled.	lockout-disabled	Windows NT
		Lockout Duration Insufficient	nt-lock-duration	Windows NT
		Lockout Window Insufficient	nt-lock-window	Windows NT
		Maximum Password Age Incorrect	nt-maxage	Windows NT
		Minimum Password Age Incorrect	nt-minage	Windows NT
		Password History Length Insufficient	nt-pw-history	Windows NT
		Windows NT Minimum Password Length	nt-pwlen	Windows NT
Total Vulnerabilities: 272				

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

Appendix B – Initial User – Desktop Workstation Scan Report

Workstation Vulnerabilities Report

Report Date: **6/23/2001 3:17:51 PM**

Policy:
User - Desktop Workstation

Comment:
Initial Scan

Scan Date:
6/23/2001 3:13:43 PM

Completion Status: ☒

Report Description:

This report displays a summary of the workstation's security vulnerabilities. Vulnerabilities are classified as having High, Medium, and Low severity. High risk vulnerabilities are those which provide unauthorized access to your workstation. Medium risk vulnerabilities are those which provide access to sensitive data on your workstation, and which may lead to the exploitation of higher risk vulnerabilities. Low risk vulnerabilities are those that provide access to potentially sensitive information.

Vulnerabilities (from High to Low severity):

Vulnerability:
User never logged on

Severity: Low

Description:
The shown user has never logged on. If this is a new account, you may ignore the message. If it is an old account, it should be considered dormant.

Fix:
Set the user's password to expire in 42 days.

Assign the user's password as follows:

1. From the **Start** menu, choose **Programs**, **Administrative Tools (Common)**, **User Manager**.
2. Select the account.
3. From the **User** menu, choose **Delete**.
4. Verify by clicking **OK**.

Additional Info:
johndoe

© SANS Institute ull rights.

© SANS Institute 2000 - 2005, Author retains full rights.

Appendix C - User Desktop Workstation Vulnerabilities

Exploit Group	Exploit	Vulnerability Name	Vulnerability ID	OS Affected
Backdoor (1)	NetBus (1)	NetBus Installed	win-netbus-installed	Windows 95,Windows 98,Windows NT
Browser (26)	Internet Explorer (19)	IE Embed bug	ie-embed	Windows 95,Windows NT
		IE mk bug	iemk-bug	Windows 95,Windows NT
		Internet Explorer vulnerability	ie-ver	Windows 95,Windows NT
		The Java Script patch is not applied	java-script-patch	Windows 95,Windows 98,Windows NT
		URL Security Zone scripting safe Active X controls.	zone-safe-scripting	Windows 95,Windows NT
		URL Security Zone Signed Active X download	zone-signed-download	Windows 95,Windows NT
		URL Security Zone Unsigned Active X download.	zone-unsigned-download	HPUX,Windows 95,Windows NT
		URL Security Zone scripting of unsafe Active X controls.	zone-unsafe-scripting	Windows 95,Windows NT
		URL Security Zone Active X execution	zone-activeX-execution	Windows 95,Windows NT
		URL Security Zone scripting safe Active X controls.	zone-safe-scripting	Windows 95,Windows NT
		URL Security Zone Auto user authentication	zone-auto-authenticate	Windows 95,Windows NT
		URL Security Zone file download	zone-file-download	Windows 95,Windows NT
		URL Security Zone low java permissions	zone-low-java	Windows 95,Windows NT
		URL Security Zone low channel permissions	zone-low-channel	Windows 95,Windows NT
		URL Security Zone file launch	zone-file-launch	Windows 95,Windows NT
		URL Security Zone desktop install	zone-desktop-install	Windows 95,Windows NT
		URL Security Zone non-secure form submission	zone-form-submission	Windows 95,Windows NT
		URL Security Zone java scripting	zone-java-scripting	Windows 95,Windows NT
		URL Security Zone active scripting	zone-active-scripting	Windows 95,Windows NT
	Netscape Navigator (7)	Netscape Navigator is outdated	nav-outdated	Windows 95,Windows NT:4.0

© SANS Institute 2000 - 2005 Author retains full rights.

		Netscape Navigator entering a secure site warning is disabled.	nav-enter-secure-site	Windows 95,Windows NT:4.0
		Netscape Navigator non-secure form submission warning is disabled.	nav-non-secure-submission	Windows 95,Windows NT:4.0
		Netscape Navigator has JavaScript enabled.	nav-javascript-enabled	Windows 95,Windows NT:4.0
		Netscape Navigator leaving a secure site warning is disabled.	nav-leave-secure-site	Windows 95,Windows NT:4.0
		Netscape Navigator mixed document security warning is disabled.	nav-mixed-doc	Windows 95,Windows NT:4.0
		Netscape Navigator has Java Enabled.	nav-java-enabled	Windows 95,Windows NT:4.0
	User checks	User Account Has Blank Password	nt-accountblankpw	Windows NT
		User Account Has a Password the Same as the Account Name	nt-accountuserpw	Windows NT
		NT Administrator Has Blank Password	nt-adminblankpw	Windows NT
		Administrator Account Has Password The Same As The Account Name	nt-adminuserpw	Windows NT
		Guessed Windows NT Administrator Password	nt-guess-admin	Windows NT
		Guessed Windows NT Guest Password	nt-guess-guest	Windows NT
		Guessed Windows NT Account Password	nt-guess-user	Windows NT
		NT Guest User Has Blank Password	nt-guestblankpw	Windows NT
		Guest Account Has a Password the Same as the Account Name	nt-guestuserpw	Windows NT
		A new user was added	nt-newuser	Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

A user has can change callback number	nt-user-changedialin	Windows NT
A user has Dialin permission	nt-user-dialin	Windows NT
A user account is dormant	nt-user-dormant	Windows NT
User never logged on	nt-user-neverloggedon	Windows NT
A user has no password	nt-nopw	Windows NT
A user's password never expires	nt-user-pwnoexpire	Windows NT
Inappropriate User with Act as System Privilege	nt-act-system	Windows NT
Inappropriate User with Add Workstation Privilege	nt-add-workstation	Windows NT
Inappropriate User with Backup Privilege	nt-backup	Windows NT
Inappropriate User with Change System Time Privilege	nt-system-time	Windows NT
Inappropriate User with Create Pagefile Privilege	nt-create-pagefile	Windows NT
Inappropriate User with Create Permanent Object Privilege	nt-create-object	Windows NT
Inappropriate User with Create Token Name Privilege	nt-create-token	Windows NT
Inappropriate User with Debug Privilege	nt-debug	Windows NT
Inappropriate User with Generate Security Audit Privilege	nt-sec-audit	Windows NT
Inappropriate User with Increase Priority Privilege	nt-increase-priority	Windows NT
Inappropriate User with Increase Quota Privilege	nt-increase-quota	Windows NT
Inappropriate User with Load Driver Privilege	nt-load-driver	Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

		Inappropriate User with Lock Memory Privilege	nt-lock-memory	Windows NT
		Inappropriate User with Profile Single Process Privilege	nt-single-process	Windows NT
		Inappropriate User with Profile System Privilege	nt-profile-system	Windows NT
		Inappropriate User with Remote Shutdown Privilege	nt-remote-shutdown	Windows NT
		Inappropriate User with Replace Process Token Privilege	nt-replace-token	Windows NT
		Inappropriate User with Restore Privilege	nt-restore	Windows NT
		Inappropriate User with System Environment Privilege	nt-system-env	Windows NT
		Inappropriate User with Take Ownership Privilege	nt-take-owner	Windows NT
		Inappropriate User with Unsolicited Input Privilege	nt-unsol-input	Windows NT
	Virus Scanner (1)	No Anti-virus Software Installed.	no-antivirus-installed	Windows 95,Windows NT
Remote Access (10)	Modems (4)	A modem was found	nt-found-modem	Windows NT
		A modem configured for AutoAnswer was found	nt-modem-autoanswer	Windows 95,Windows NT
		A modem configured for AutoAnswer was found and Dial Tone was detected on the phone line	nt-modem-dialtone	Windows 95,Windows NT
		A modem may be on the specified COM port	nt-possible-modem	Windows NT
	pcANYWHERE32 (1)	pcANYWHERE32 is installed	pcanywhere32-installed	Windows 95,Windows NT
	Carbon Copy 32 (1)	Carbon Copy 32 is installed	carboncopy32-installed	Windows 95,Windows NT
	Remotely Possible/32 (1)	Remotely Possible/32 is installed	remotelypossible32-installed	Windows 95,Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

	LapLink (2)	LapLink is installed	laplink-installed	Windows 95,Windows NT
		Remote DeskLink for Windows 95 is installed	remote-desklink-installed	Windows 95
	RAS (1)	Found a RAS port configured to receive calls	nt-ras-dialin	Windows NT
Total Vulnerabilities: 75				

© SANS Institute 2000 - 2005, Author retains full rights.

Appendix B – Initial User – Desktop Workstation Scan Report

Workstation Vulnerabilities Report

Report Date: **6/23/2001 3:17:51 PM**

Policy:
User - Desktop Workstation

Comment:
Initial Scan

Scan Date:
6/23/2001 3:13:43 PM

Completion Status: ☒

Report Description:

This report displays a summary of the workstation's security vulnerabilities. Vulnerabilities are classified as having High, Medium, and Low severity. High risk vulnerabilities are those which provide unauthorized access to your workstation. Medium risk vulnerabilities are those which provide access to sensitive data on your workstation, and which may lead to the exploitation of higher risk vulnerabilities. Low risk vulnerabilities are those that provide access to potentially sensitive information.

Vulnerabilities (from High to Low severity):

Vulnerability:
User never logged on

Severity: Low

Description:
The shown user has never logged on. If this is a new account, you may ignore the message. If it is an old account, it should be considered dormant.

Fix:
Set the user's password to expire in 42 days.

Assign the user's password as follows:

5. From the **Start** menu, choose **Programs**, **Administrative Tools (Common)**, **User Manager**.
6. Select the account.
7. From the **User** menu, choose **Delete**.
8. Verify by clicking **OK**.

Additional Info:
johndoe

© SANS Institute ull rights.

© SANS Institute 2000 - 2005, Author retains full rights.

Appendix C - User Desktop Workstation Vulnerabilities

Exploit Group	Exploit	Vulnerability Name	Vulnerability ID	OS Affected
Backdoor (1)	NetBus (1)	NetBus Installed	win-netbus-installed	Windows 95,Windows 98,Windows NT

Browser (26)	Internet Explorer (19)	IE Embed bug	ie-embed	Windows 95,Windows NT
		IE mk bug	iemk-bug	Windows 95,Windows NT
		Internet Explorer vulnerability	ie-ver	Windows 95,Windows NT
		The Java Script patch is not applied	java-script-patch	Windows 95,Windows 98,Windows NT
		URL Security Zone scripting safe Active X controls.	zone-safe-scripting	Windows 95,Windows NT
		URL Security Zone Signed Active X download	zone-signed-download	Windows 95,Windows NT
		URL Security Zone Unsigned Active X download.	zone-unsigned-download	HPUX,Windows 95,Windows NT
		URL Security Zone scripting of unsafe Active X controls.	zone-unsafe-scripting	Windows 95,Windows NT
		URL Security Zone Active X execution	zone-activeX-execution	Windows 95,Windows NT
		URL Security Zone scripting safe Active X controls.	zone-safe-scripting	Windows 95,Windows NT
		URL Security Zone Auto user authentication	zone-auto-authenticate	Windows 95,Windows NT
		URL Security Zone file download	zone-file-download	Windows 95,Windows NT
		URL Security Zone low java permissions	zone-low-java	Windows 95,Windows NT
		URL Security Zone low channel permissions	zone-low-channel	Windows 95,Windows NT
		URL Security Zone file launch	zone-file-launch	Windows 95,Windows NT
		URL Security Zone desktop install	zone-desktop-install	Windows 95,Windows NT
		URL Security Zone non-secure form submission	zone-form-submission	Windows 95,Windows NT
		URL Security Zone java scripting	zone-java-scripting	Windows 95,Windows NT
		URL Security Zone active scripting	zone-active-scripting	Windows 95,Windows NT
	Netscape Navigator (7)	Netscape Navigator is outdated	nav-outdated	Windows 95,Windows NT:4.0
		Netscape Navigator entering a secure site warning is disabled.	nav-enter-secure-site	Windows 95,Windows NT:4.0

© SANS Institute 2000 - 2005 Author retains full rights.

		Netscape Navigator non-secure form submission warning is disabled.	nav-non-secure-submission	Windows 95,Windows NT:4.0
		Netscape Navigator has JavaScript enabled.	nav-javascript-enabled	Windows 95,Windows NT:4.0
		Netscape Navigator leaving a secure site warning is disabled.	nav-leave-secure-site	Windows 95,Windows NT:4.0
		Netscape Navigator mixed document security warning is disabled.	nav-mixed-doc	Windows 95,Windows NT:4.0
		Netscape Navigator has Java Enabled.	nav-java-enabled	Windows 95,Windows NT:4.0
	User checks	User Account Has Blank Password	nt-accountblankpw	Windows NT
		User Account Has a Password the Same as the Account Name	nt-accountuserpw	Windows NT
		NT Administrator Has Blank Password	nt-adminblankpw	Windows NT
		Administrator Account Has Password The Same As The Account Name	nt-adminuserpw	Windows NT
		Guessed Windows NT Administrator Password	nt-guess-admin	Windows NT
		Guessed Windows NT Guest Password	nt-guess-guest	Windows NT
		Guessed Windows NT Account Password	nt-guess-user	Windows NT
		NT Guest User Has Blank Password	nt-guestblankpw	Windows NT
		Guest Account Has a Password the Same as the Account Name	nt-guestuserpw	Windows NT
		A new user was added	nt-newuser	Windows NT
		A user has can change callback number	nt-user-changedialin	Windows NT
		A user has Dialin permission	nt-user-dialin	Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

A user account is dormant	nt-user-dormant	Windows NT
User never logged on	nt-user-neverloggedon	Windows NT
A user has no password	nt-nopw	Windows NT
A user's password never expires	nt-user-pwnoexpire	Windows NT
Inappropriate User with Act as System Privilege	nt-act-system	Windows NT
Inappropriate User with Add Workstation Privilege	nt-add-workstation	Windows NT
Inappropriate User with Backup Privilege	nt-backup	Windows NT
Inappropriate User with Change System Time Privilege	nt-system-time	Windows NT
Inappropriate User with Create Pagefile Privilege	nt-create-pagefile	Windows NT
Inappropriate User with Create Permanent Object Privilege	nt-create-object	Windows NT
Inappropriate User with Create Token Name Privilege	nt-create-token	Windows NT
Inappropriate User with Debug Privilege	nt-debug	Windows NT
Inappropriate User with Generate Security Audit Privilege	nt-sec-audit	Windows NT
Inappropriate User with Increase Priority Privilege	nt-increase-priority	Windows NT
Inappropriate User with Increase Quota Privilege	nt-increase-quota	Windows NT
Inappropriate User with Load Driver Privilege	nt-load-driver	Windows NT
Inappropriate User with Lock Memory Privilege	nt-lock-memory	Windows NT
Inappropriate User with Profile Single Process Privilege	nt-single-process	Windows NT

© SANS Institute 2000 - 2005 Author retains full rights.

		Inappropriate User with Profile System Privilege	nt-profile-system	Windows NT
		Inappropriate User with Remote Shutdown Privilege	nt-remote-shutdown	Windows NT
		Inappropriate User with Replace Process Token Privilege	nt-replace-token	Windows NT
		Inappropriate User with Restore Privilege	nt-restore	Windows NT
		Inappropriate User with System Environment Privilege	nt-system-env	Windows NT
		Inappropriate User with Take Ownership Privilege	nt-take-owner	Windows NT
		Inappropriate User with Unsolicited Input Privilege	nt-unsol-input	Windows NT
	Virus Scanner (1)	No Anti-virus Software Installed.	no-antivirus-installed	Windows 95,Windows NT
Remote Access (10)	Modems (4)	A modem was found	nt-found-modem	Windows NT
		A modem configured for AutoAnswer was found	nt-modem-autoanswer	Windows 95,Windows NT
		A modem configured for AutoAnswer was found and Dial Tone was detected on the phone line	nt-modem-dialtone	Windows 95,Windows NT
		A modem may be on the specified COM port	nt-possible-modem	Windows NT
	pcANYWHERE32 (1)	pcANYWHERE32 is installed	pcanywhere32-installed	Windows 95,Windows NT
	Carbon Copy 32 (1)	Carbon Copy 32 is installed	carboncopy32-installed	Windows 95,Windows NT
	Remotely Possible/32 (1)	Remotely Possible/32 is installed	remotelypossible32-installed	Windows 95,Windows NT
	LapLink (2)	LapLink is installed	laplink-installed	Windows 95,Windows NT
		Remote DeskLink for Windows 95 is installed	remote-desklink-installed	Windows 95

© SANS Institute 2000 - 2005 Author retains full rights.

	RAS (1)	Found a RAS port configured to receive calls	nt-ras-dialin	Windows NT
Total Vulnerabilities: 75				

© SANS Institute 2000 - 2005, Author retains full rights.

References

Schneier, Bruce. “Opinion: The importance of vigilance.” 4 Apr. 2000. URL:http://www.zdnet.com/filters/printerfriendly/0,6061,2510681-107,00.html (8 June 2001)

Genusa, Angela. “12 Keys for Locking Up Tight.” 1 Mar. 2001. URL:http://www2.cio.com/archive/030101/keys_content.html (8 June 2001)

“Windows 2000 Security Installation Checklist.” 31 May 2001. URL:http://www.labmice.net/articles/securingwin2000.htm (11 June 2001)

Smith, Randy Franklin. “Audit Account Logon Events.” Windows 2000 Magazine. Mar. 2001. URL:http://www.win2000mag.com/Articles/Print.cfm?ArticleID=19677 (01 June 2001)

Cox, Philip. Windows 2000 Security Handbook. Osborne/McGraw-Hill, 2000.

Millican, John. “GCNT Certification Practical.” 7 April 2001.

Jumes, James; Cooper, Neil; Chamoun, Paula; Feinman, Todd. Microsoft Windows NT 4.0 Security, Audit and Control. Microsoft Press, 1998.

Sjouwerman, Stu; Shilmover, Barry; Stewart, Michael. Windows 2000 System Administrator’s Black Book. Scottsdale: The Coriolis Group, 2000.

23 May 2001. http://cve.mitre.org/about/terminology.html (24 June 2001)

23 May 2001. http://cve.mitre.org/ (24 June 2001)

ISS. “System Scanner Getting Started Guide” File://D:\Program Files\ISS\SysScan\Documentation\get started.pdf.

© SANS Institute 2000 - 2005, Author retains full rights.