Global Information Assurance Certification Paper

SANS GIAC

Securing Windows
GCNT Practical Assignment

Version 2.1

Windows 2000 Resource Kit Tool
System Scanner 1.1
Tutorial

Deborah R. Dean

TABLE OF CONTENTS

1. INTRODUCTION 1
   1.1 Purpose 1

2. INSTALLATION 3
   2.1 System Requirements 3
      2.1.1 Win NT Requirements 3
      2.1.2 NT Server Requirements 3
      2.1.3 Windows 2000 Requirements 4
   2.2 Location of Files 4
   2.3 Installation Procedure 4

3. OPERATION OF SOFTWARE 6
   3.1 Default System Scan 6
      3.1.1 Correcting Vulnerabilities Detailed During Default Scan 8
      3.1.1.1 Method One 8
      3.1.1.2 Method Two 9
      3.1.2 Reset Baseline for the Scan Policy 11
      3.1.3 Run Scans Again Using the "Desktop Workstation" Policy 12
      3.1.4 Continue Steps 3.1 – 3.1.4 Until System is Free of all Vulnerabilities 13
      3.1.5 Additional Testing Using Different Policies 13
      3.1.6 Types of Default Policies 13
   3.2 Create Policies to Further Customize System Scanner 1.1 14
      3.2.1 Automatic Policy Creation 14
      3.2.2 Manual Policy Creation 15
      3.2.3 Document the Security Status of the System 15
   3.3 Baseline Databases 16
      3.3.1 Share Scan Baseline 16
      3.3.2 User Scan Baseline 16
      3.3.3 Group Scan Baseline 16
      3.3.4 Services Baseline 16
      3.3.5 File scan Baseline 16
      3.3.6 Registry Baseline 17
      3.3.7 Process Baseline 17
   3.4 Reports 17
      3.4.1 Vulnerabilities Report 18
      3.4.2 Services Report 18
      3.4.3 Trends Report 19
      3.4.4 Differential Report 20
   3.5 Scheduled Scans 21
      3.5.1 How to Schedule a Scan 22

3.5.2 Running a Scan in Background Mode 22
4. SECURITY PRACTICES 23
5. FEATURES AND BENEFITS 23
6. POTENTIAL DRAWBACKS AND SHORTCOMINGS 24
7. CONCLUSION 25
8. REFERENCES 25
9. ACRONYMS 25

LIST OF FIGURES

Figure 2.3-1: Setup Screen 5
Figure 2.3-2 System Scanner 1.1 Folder Location 5
Figure 2.3-3 Setup Welcome Screen 6

Figure 3.1-1 Default System Scan 6
Figure 3.1-2 Scan Now Box 7
Figure 3.1-3 Scan Complete 7
Figure 3.1.1.1-1 The "What's This" Box 8
Figure 3.1.1.1-2 Vulnerability Correction Mode 9
Figure 3.1.1.2-1 Vulnerabilities Report Menu 10
Figure 3.1.3.2-2 Sample Vulnerability Report 11
Figure 3.1.2-1 Baseline Reset 12
Figure 3.1.2-2 Baseline Reset Selection 12
Figure 3.2.1-1 New Policy Wizard 14
Figure 3.2.2-1 Settings for Manual Policy Creation 15
Figure 3.4-1 System Scanner 1.1 Reports 17
Figure 3.4-2 Report Screen 18
Figure 3.4.2-1 Sample Services Report 19
Figure 3.4.3-1 Sample Trends Report 20
Figure 3.4.4-1 Sample Differential Report 21
Figure 3.5.1-1 Scan Scheduling 22
Figure 3.5.2-1 Background Mode Scan 23

WINDOWS 2000 RESOURCE KIT APPLICATION TOOL SYSTEM SCANNER 1.1

1. INTRODUCTION

System Scanner 1.1 is a security assessment solution for Windows-based products that combines automated security policy management and automated implementation of security policies. This product is located on the Windows 2000 Resource Kit CD-ROM. System Scanner 1.1 provides a host-based security assessment that cannot be accomplished by network scanning. This tool is flexible and has an extensible rules-based manager/agent system for checking and managing the compliance to security policies. The System Scanner 1.1 product provided on the Resource Kit CD works on a single system. There is a licensed version available from the vendor that can test systems on a distributed network.

1.1 Purpose

System Scanner 1.1 can be used to check for nearly 300 vulnerability checks including, but not limited to:

- Comprehensive Microsoft IIS checks
- Configuration of virus scanners
- Browser-specific vulnerabilities
- Presence of well-known TCP/IP-based services
- NetBIOS checks
- Registry security checks
- Remote access checks and modem checks

System Scanner 1.1 can be used to define tailored policies, as well as schedule scans to be performed at predetermined times on the system. This package gives the system administrator the ability to scan systems, assistance in correcting the vulnerabilities found, and create reports that can be used to track the security posture of the system.

Because this version of System Scanner 1.1 operates from within the host that it is scanning, it can access file permissions, determine file ownership, test network service configurations, review account setup, verify which security patches were installed, identify vulnerable programs loaded on the system, and identify many common user-related security weaknesses that non-hosted software cannot.

System Scanner 1.1 scans for security holes that can place systems at risk. It also provides assistance in reducing the identified risks. System Scanner 1.1 uses the following groups of checks:

- Internet Protocol Checks
  - Services Scan
  - FTP
- Browser Checks
  - Internet Explorer
  - Netscape
- Operating System Checks
  - Denial of Service (DoS)
  - OS Version
  - Internet Information Server (IIS)
  - Password Settings
  - Registry Settings
  - User Checks
  - Share Checks
  - NetBIOS
- Applications Checks
  - Microsoft (MS) Office
  - Virus Scanner
  - pcANYWHERE32
  - CarbonCopy32
  - Remote Possible / 32
  - LapLink
- Baseline Checks
  - Registry Scan
  - File Scan
  - Services
  - Processes
  - User Scans
  - Group Scans
  - Share Scans
- Remote Access Checks
  - Modem
  - Remote Access Server (RAS)

2. INSTALLATION

System Scanner 1.1 is not part of the normal Windows 2000 operating system load and is not installed during the automatic Windows 2000 Resource Kit installation. This product requires manual installation by someone with system administrator rights as shown in Section 2.3.

When installing System Scanner 1.1 on an NTFS directory, the install process sets permissions so only system administrators have full access to all files. The install directory and registry keys for this program are locked down. ISS (the product vendor) recommends that the default permissions set by System Scanner 1.1 during the install not be changed or removed.

2.1 System Requirements

System Scanner 1.1 is for MS Windows based systems and runs on Microsoft's Windows 9x, Windows NT and Windows 2000 operating systems. The file that is installed is approximately 15 MB in size.

2.1.1 Win NT Requirements

Required
- Pentium class processor
- 8 MB RAM
- 25 MB disk space
- TCP/IP installed

Recommended
- Pentium class processor
- 32 MB RAM
- 32 MB disk space
- TCP/IP installed

2.1.2 NT Server Requirements

Required
- Pentium class processor
- 16 MB RAM
- 25 MB disk space
- TCP/IP installed

Recommended
- Pentium class processor
- 32 MB RAM
- 32 MB disk space
- TCP/IP installed

2.1.3 Windows 2000 Requirements

Required
- Pentium class processor
- 32 MB RAM
- 25 MB disk space
- TCP/IP installed

Recommended
- Pentium class processor
- 64 MB RAM
- 35 MB disk space
- TCP/IP installed

2.2 Location of Files

All required files for installation of System Scanner 1.1 are located in on the **Windows 2000 Resource Kit CD-ROM** in the **\apps\systemsscanner** folder.

2.3 Installation Procedure

The following steps are used to install the file:

a. Insert the Windows 2000 Resource Kit companion CD-ROM into the CD-ROM drive.

b. When the Setup screen appears, click **Explore the CD** (if autorun is not enabled, use the standard “My Computer” and explore the Windows 2000 Resource Kit CD and go o the \apps\systemscanner folder).

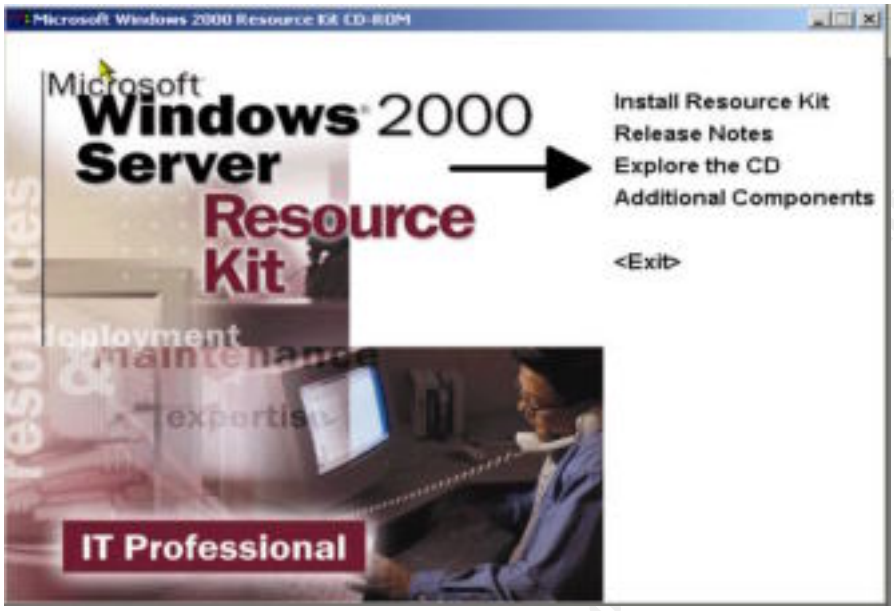

Figure 2.3-1: Setup Screen

c. In the \apps\systemscanner folder, double click the file **Sysscansetup.exe**.

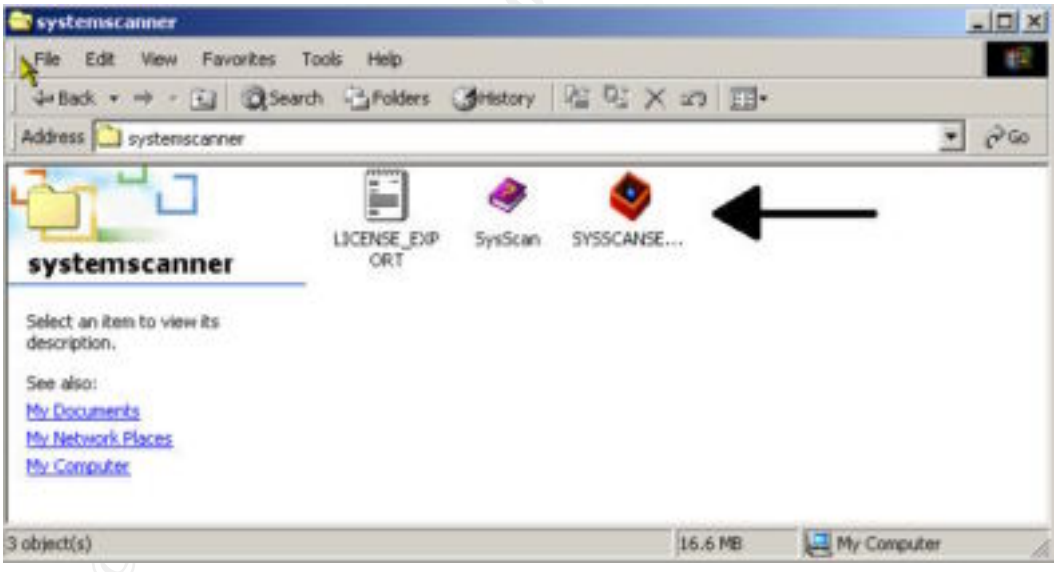

Figure 2.3-2 System Scanner 1.1 Folder Location

d. From that point, follow the directions on the screen.

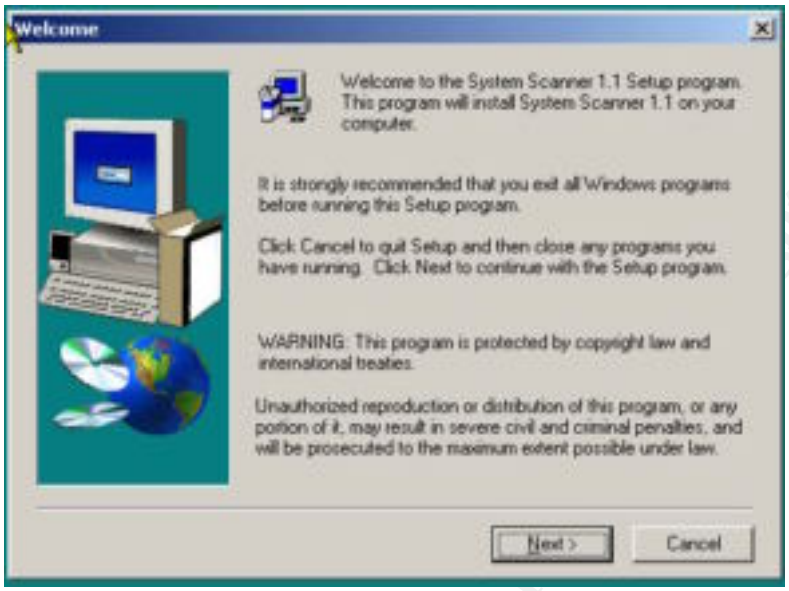

Figure 2.3-3 Setup Welcome Screen

3. OPERATION OF SOFTWARE

Once System Scanner 1.1 has been installed on the system, click **Start**, then point to **Programs**, open **ISS**, and then click on **System Scanner Help**. The help files will provide specific information about the program. It is important that these help files be viewed before starting the program. To run the program, click **Start**, **Programs**, **ISS** and then **System Scanner 1.1.**

3.1 Default System Scan

It is recommended that the first thing to do, once System Scanner 1.1 is installed, is to run a default scan on the system for vulnerabilities. To run this default scan, follow these steps:

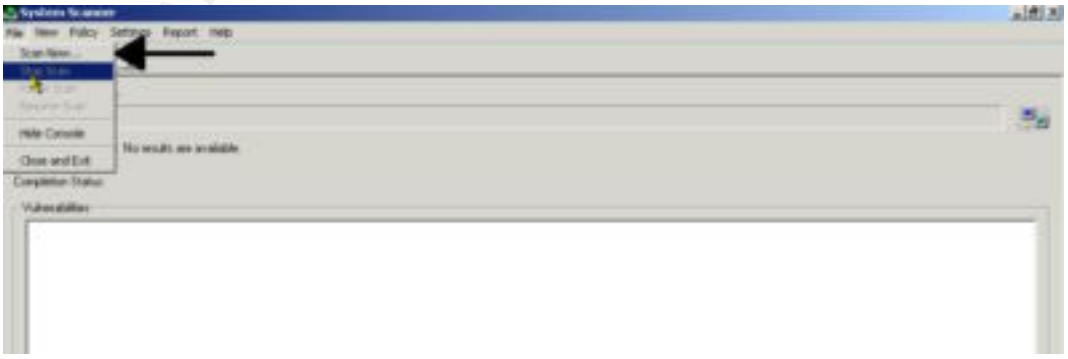

Figure 3.1-1 Default System Scan

Click **File, Scan Now**. A “scan now” box will pop up. At this point a pull-down selection box is available for selecting a "Policy to use". Choose the policy from the pull-down box that most closely matches a description of the type of system or application that the system runs. Then click **OK**. The next screen shows a bar with the overall scan process, current scan started date and time, the policy that was chosen, and a list of vulnerabilities that System Scanner 1.1 found.

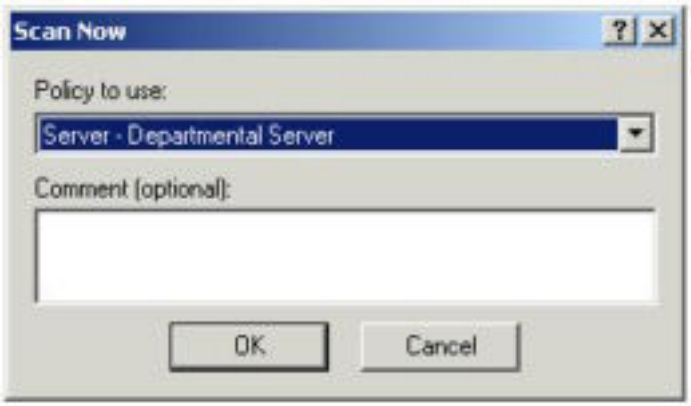

Figure 3.1-2 Scan Now Box

This page will also display the number of high, medium, and low vulnerabilities that were found on the system during the scan. Once the scan is completed, a completion box will appear, click **OK**.

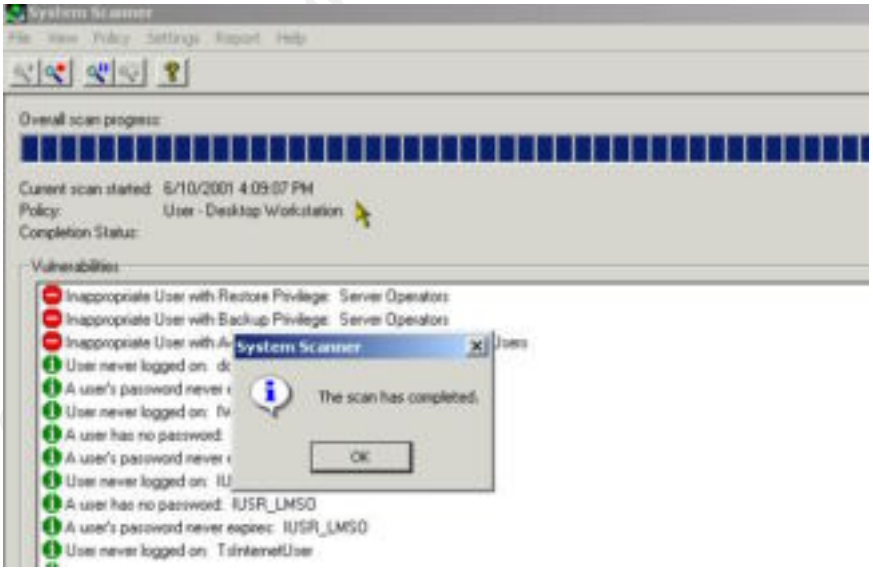

Figure 3.1-3 Scan Complete

When the scan is finished the next thing to be done is to identify vulnerabilities and then correct them.

3.1.1 Correcting Vulnerabilities Detailed During Default Scan

There are two (2) methods in which vulnerabilities can be viewed. System Scanner 1.1 provides a mode of correction for vulnerabilities in either method. The difference in the two methods is that one method views a single vulnerability and its correction at a time while the second method generates a report of all vulnerabilities in one report. Each of the two methods is described in detail below.

3.1.1.1 Method One

Method One is a way of looking at each individual vulnerability that is listed in the vulnerability list within System Scanner 1.1. This method only allows the ability to view one vulnerability and its corrective mode at a time.

Right click on one of the vulnerabilities. A **"What's This?"** box will pop up. Click on the box and a detail description of the vulnerability, risk priority, OS vulnerability, and a mode of correction will appear.

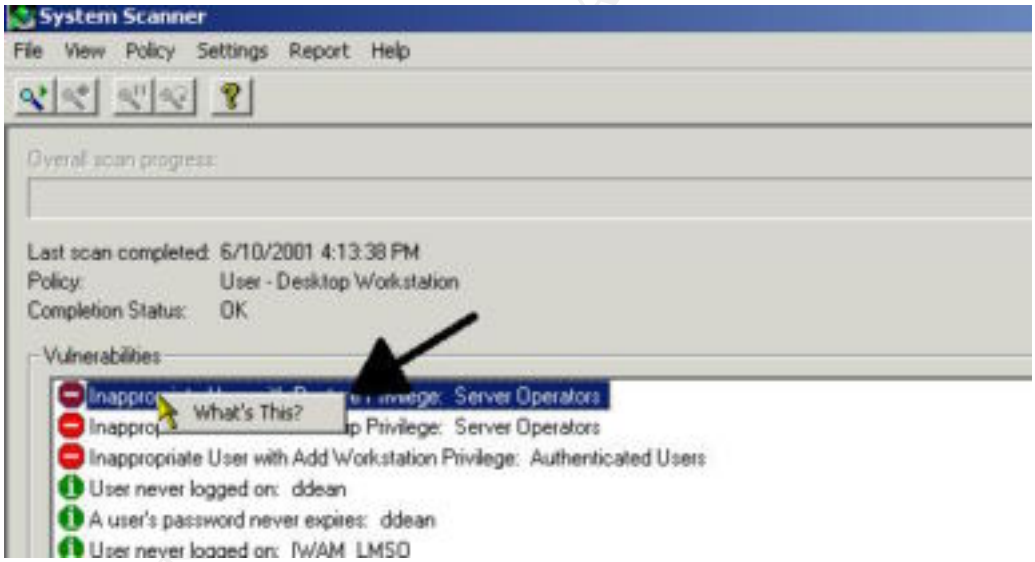

Figure 3.1.1.1-1 The "What's This" Box

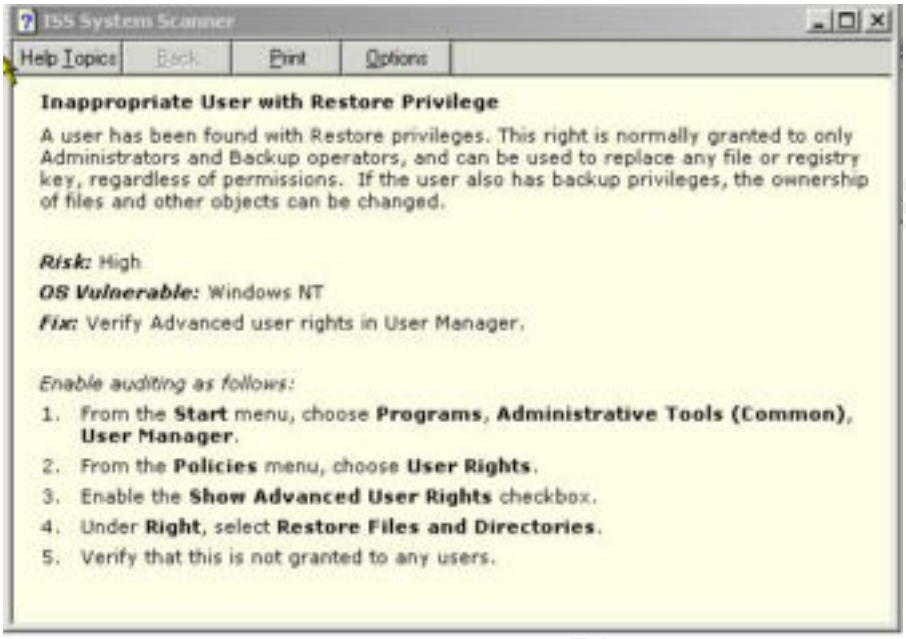

Figure 3.1.1.1-2 Vulnerability Correction Mode

Vulnerabilities should be corrected immediately after a scan is complete. Correcting the vulnerabilities that are found may require a number of different skills and knowledge of a variety of tools and techniques. System Scanner 1.1 provides a step-by-step procedure for each identified vulnerability. An example is shown in Figure 3.1.1.1-2.

- Editing the registry – to edit the registry in Windows NT, use **regedit32.exe**, and for Windows 95, use **regedit.exe**. It should be noted that using the Registry Editor incorrectly could result in system-wide problems that may require the reinstallation of the operating system.
- Applying patches – these are executable programs provided by the software vendor to correct bugs in the software.
- Setting file permissions – file permissions are set to correct system related vulnerabilities
- Running the User Manager (Windows NT) - user manager is used to correct vulnerabilities related to users and groups.
- Running the Policy Editor (Win 95 and 98) – policy editor is used to correct such things as access control, logon settings, password settings, etc.

Each vulnerability identified in the list should be addressed. Once this has been completed, reset the system baseline as described in Section 3.1.2.

3.1.1.2 Method Two

Method Two will allow the generation a vulnerability report that will show all of the vulnerabilities and their mode of correction at once. This method allows the ability to

print this report and correct all the vulnerabilities without having to go to each one individually.

To view the Vulnerability Report:

- From **Report** menu, choose **Vulnerability**
- Under **Scans**, select the scan to be viewed.
- Under **Vulnerability Severity**, enable **High, Medium,** or **Low Risk**.
- Under **Report Detail**, enable either **Full Description**, **Fix Information**, or **Policy Info**.
- Click **Next**.
- Click on **View the report in your web browser**.
- Click **Finish**.

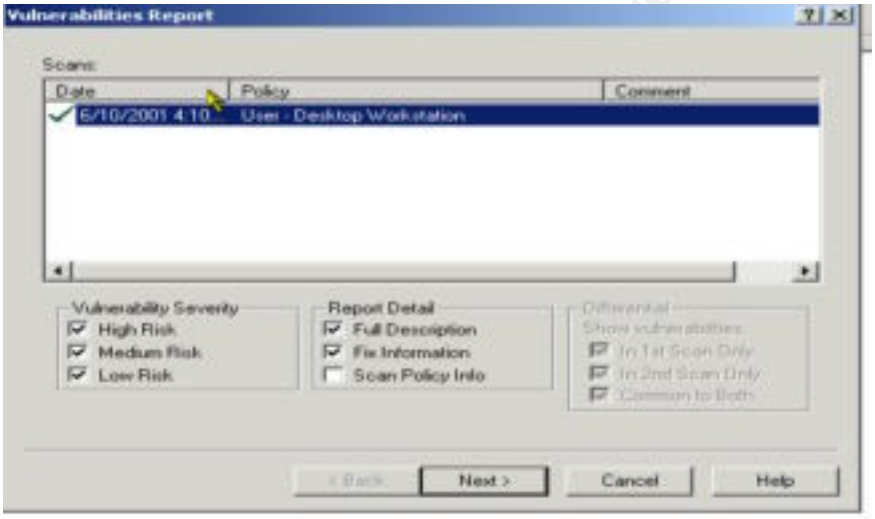

Figure 3.1.1.2-1 Vulnerabilities Report Menu

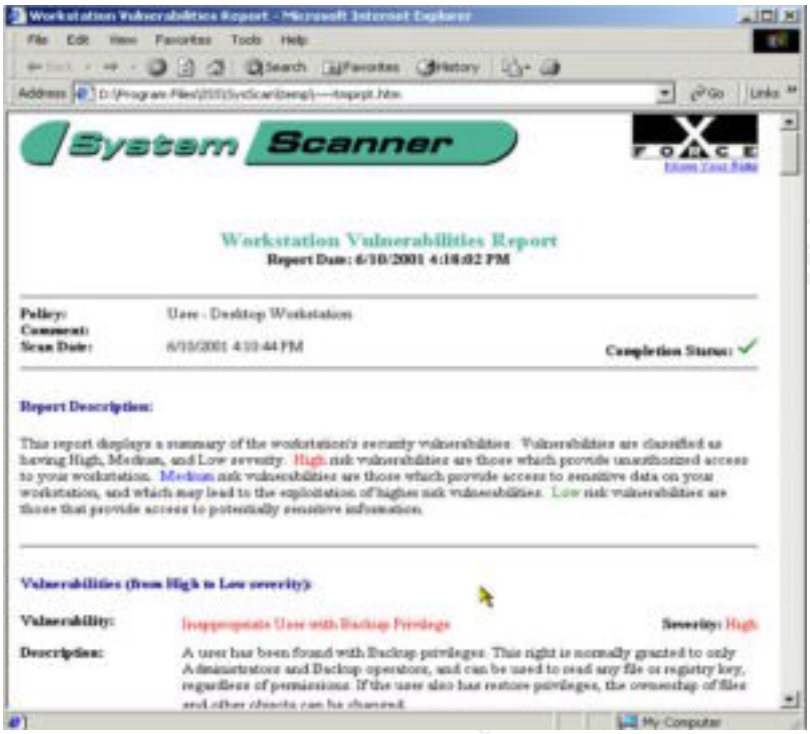

Figure 3.1.3.2-2 Sample Vulnerability Report

3.1.2 Reset Baseline for the Scan Policy

Resetting the scan policy baseline is necessary in order to update the database to the new system configuration and to prevent the next scan from detecting the changes to the system as intrusions or new vulnerabilities. This product, once the original baseline is established, will detect changes to key system parameters and report them as vulnerabilities until the baseline is reset. To prevent the corrections from being identified as intrusions reset the baseline as follows:

Click **Policy**, **Reset Baseline**, choose the policy and check all the baselines that need to be reset.

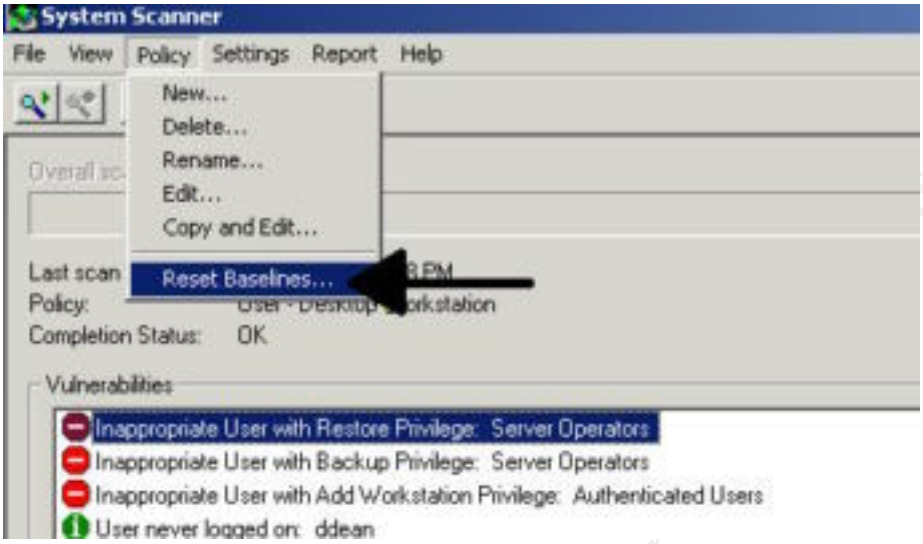

Figure 3.1.2-1 Baseline Reset

Click **Reset**, **Close**. At this point all baselines are reset to the new configuration of the system.

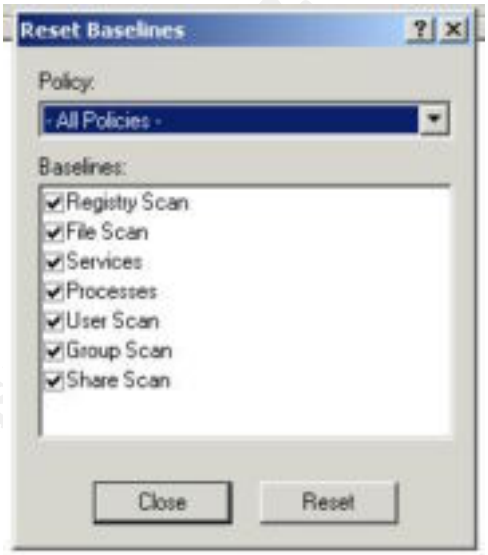

Figure 3.1.2-2 Baseline Reset Selection

3.1.3 Run Scans Again Using the "Desktop Workstation" Policy

After the baseline has been reset, run the scan again using the desktop workstation policy to insure that all the vulnerabilities have been corrected properly.

3.1.4 Continue Steps 3.1 – 3.1.4 Until System is Free of all Vulnerabilities

If there are remaining or new vulnerabilities shown after running the scanner again, repeat steps 3.1 – 3.1.4 until the system is free from all vulnerabilities. Once the system is completely free from all vulnerabilities remember to reset the baseline database.

3.1.5 Additional Testing Using Different Policies

This product has the ability to be customized for different system configurations or exposures to a varying level of threats by selecting another default policy from several provided or by creating a custom scan policy. This allows for the scanner to be optimized based on the actual system configuration and environment.

3.1.6 Types of Default Policies

ISS System Scanner 1.1 comes with several default policies to use for scanning your system. A policy is a group of checks that are run during a scan. Policies can be created manually or one of several predefined policies within System Scanner 1.1 can be selected based on the needs of the system.

- User Desktop System Policies
  - Power User Desktop Workstation – This policy is designed for users who run a wide variety of power applications or utilities.
  - Desktop Workstation – This policy is designed for the typical Windows user desktop workstation.
  - Home Computer – Scans for viruses, backdoors, or software settings that can hinder the performance of home systems.
- Server System Policies
  - Departmental Server – This provides the lowest level of testing because these systems have less exposure than Intranet Servers do. Registry, NetBIOS and IIS testing are not enabled.
  - Intranet Server – These systems are usually intranet web servers behind a firewall. Since these systems are on an intranet, fewer checks are enabled, specifically DoS and virus check is not enabled.
  - DMZ FTP Server – This policy is designed for any server installed in a DMZ not running a web service. Due to the heavy exposure all vulnerabilities except web server, browser, MS Office and modems are checked.
  - DMZ Web Server – This policy is designed for any system installed in a DMZ that is running a web server. All vulnerabilities except MS Office, browser, and modem are checked.
- Technical Policies
  - Baseline Policy – With this policy the system configuration lockdown is tested.
  - Browse Only – For this policy the web browser software settings are checked.

- Services Scan – This policy checks any audit server application that is running.
- OS Lockdown Policy – Most baseline checks are enabled.
- Heavy Scan Policy – All checks are enabled for this policy scan. This scan will check the system for all vulnerabilities.

3.2 Create Policies to Further Customize System Scanner 1.1

System Scanner 1.1 allows the creation specific policies to further customize security needs. A policy must be present in order for System Scanner 1.1 to run. Below are the steps required to create a policy automatically and manually.

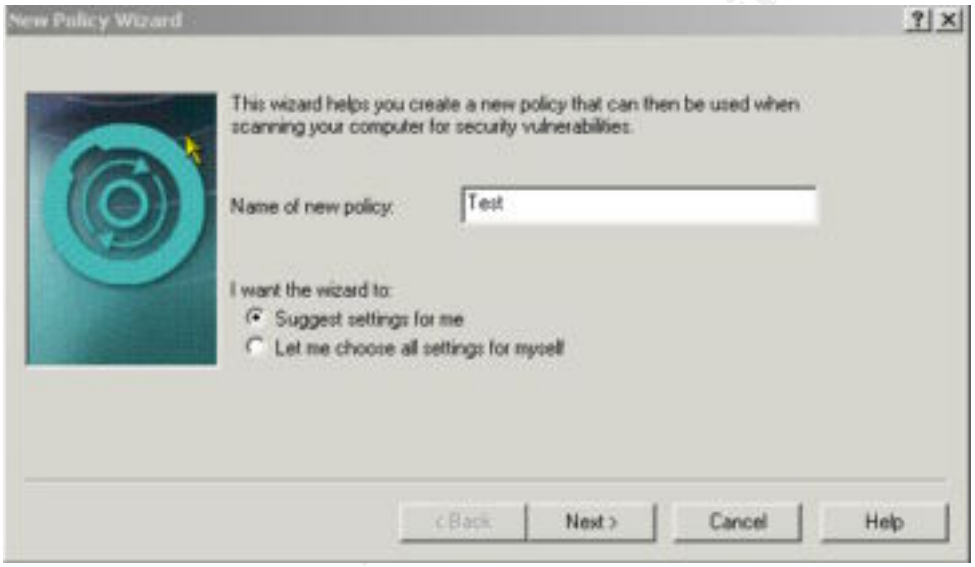

Figure 3.2.1-1 New Policy Wizard

3.2.1 Automatic Policy Creation

When using the automatic policy creation, System Scanner 1.1 will choose the setting for the system administrator.

- From the **Policy** menu click **New**. This will open the New Policy Wizard.
- Create a name for the policy in the **Name of New Policy** block.
- Under the **I Want the Wizard to** box click **Suggest Scan Settings for Me**.
- Click **Next**.
- Click **Run Smart Configuration**. A bar will show how fast the process is running.
- Click **Save the Policy without Modification**.
- Click **Finish**.

The new policy will be created and can be used the next time a scan is run on the system.

3.2.2 Manual Policy Creation

When using the manual policy creation, the system administrator chooses the appropriate settings for the type of system being scanned.

- From the **Policy** menu click **New**. This will open the New Policy Wizard.
- Create a name for the policy in the **Name of New Policy** block.
- Under the **I want Wizard to**, click **Let me choose all scan settings for myself**.
- Click **Next**.
- Select the appropriate check box on the left and configure the exploits on the right.
- Click **Finish**.

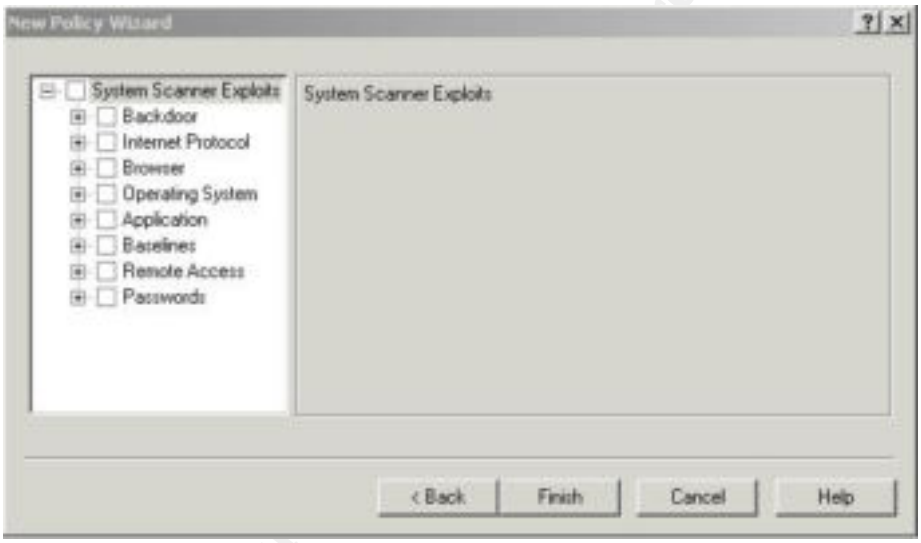

Figure 3.2.2-1 Settings for Manual Policy Creation

The new policy will be created and can be used the next time a scan is run on the system.

This feature also has the capability to edit, copy, delete, and rename policies. This is accomplished from the **Policy** menu.

3.2.3 Document the Security Status of the System

After the system has been secured using the specified policy of choice, a final vulnerability report should be generated to document the security status of the system. This is accomplished in the same method as detailed in Section 3.1.1.2, Method Two. The report will be shown as a web document that can be viewed, printed, or saved using standard browser techniques. This document will detail the following:

- The policy used
- Any comments about the scan
- Scan date and time
- Completion status
- Description of what the report displays
- Each vulnerability found (from high to low severity)
- A detailed description of the vulnerability, and
- A fix for that vulnerability.

3.3 Baseline Databases

The key component used to monitor changes in the system is the baseline database. This database keeps the information on the scans and has the ability to report if an intruder has gained access to the system and modified any files or registry keys. A baseline scan is run in order for System Scanner 1.1 to become familiar with and to store a copy of the current configuration of the system. Any change to the configuration of the system after the baseline data is stored is reported as a vulnerability.

There are several different baseline databases:

3.3.1 Share Scan Baseline

This is a "snap shot" of the system share settings, which include hidden shares, share permissions on NTFS, permissions on the share itself, and printed shares.

3.3.2 User Scan Baseline

This baseline sets the logon settings, RAS settings, and user rights. This is used to determine changes on the system related to user accounts and privileges.

3.3.3 Group Scan Baseline

This baseline sets the group rights and user rights. It determines if any group changes have been made.

3.3.4 Services Baseline

This baseline sets the systems services and device settings, which includes server applets and device applets.

3.3.5 File scan Baseline

This baseline is used to determine if any files have been changed on the system.

3.3.6 Registry Baseline

This baseline is used to identify any registry key changes on the system.

3.3.7 Process Baseline

This baseline reports changes to the common Run key in the registry, common startup folder load and run value, user specific Run key and user specific startup folder.

If the baseline is not reset after changing your system environment all those changes that were made will be reported as vulnerabilities during the next baseline scan. System Scanner 1.1's capability allows system administrators to maintain configuration methods. Review of these metrics helps identify systems that have been damaged or altered.

3.4 Reports

System Scanner 1.1 allows you to generate four types of reports. These reports are generated and viewed in html format.

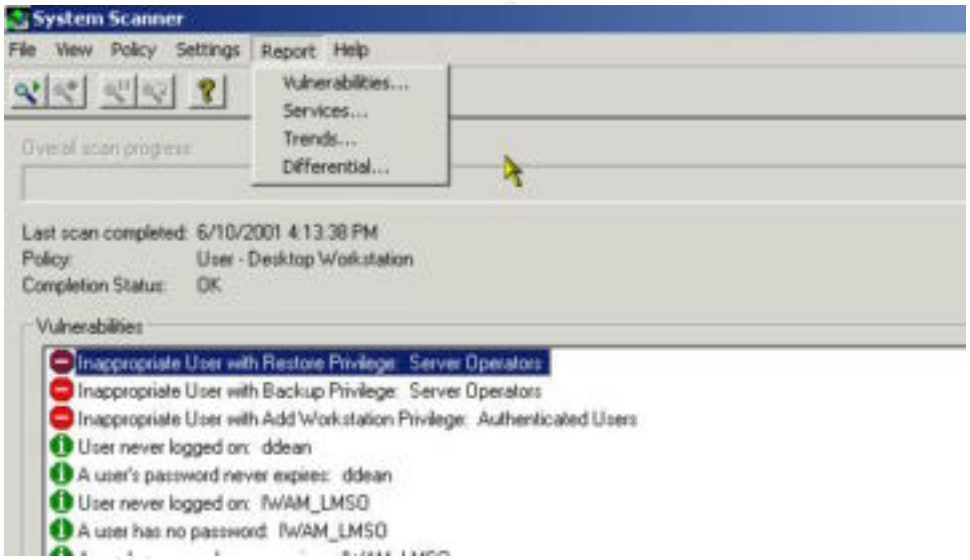

Figure 3.4-1 System Scanner 1.1 Reports

After choosing the type of report to be viewed, a list of all the scans that have been performed on the system will be shown from which to choose from.

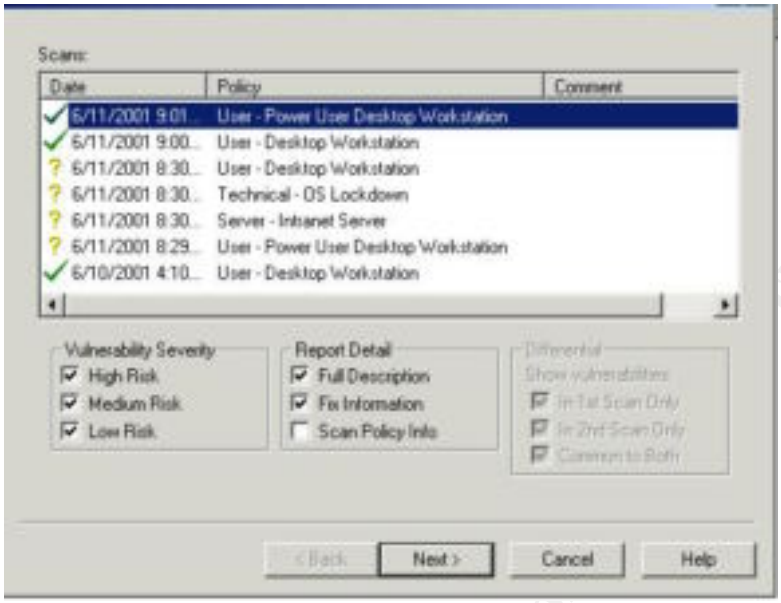

Figure 3.4-2 Report Screen

3.4.1 Vulnerabilities Report

This report shows all the vulnerabilities that were found on the system and step-by-step assessment information on the vulnerability.

To view the Vulnerability Report:

- From **Report** menu, choose **Vulnerability**
- Under **Scans**, select the scan to view.
- Under **Vulnerability Severity**, enable **High, Medium,** or **Low Risk**.
- Under **Report Detail**, enable either **Full Description**, **Fix Information**, or **Policy Info**.
- Click **Next**.
- Click on **View the report in your web browser**.
- Click **Finish**.

See Figure 3.1.3.2-1 Sample Vulnerability Report.

3.4.2 Services Report

This report shows all the services that are running on the system and which port they are running on. This report would help an administrator identify the activities of a “bot”, “zombie”, or “Trojan” on the system that may be using an external connection or exposing the system to attacks.

To view the Services Report:

- From **Report** menu, choose **Services**.
- Select the report to scan under **Scans**.
- Under **Report Detail** enable either **Full Description**, **Fix Information**, or **Policy Info**.
- Click **Next**.
- Click on **View the report in your web browser**.
- Click **Finish**.

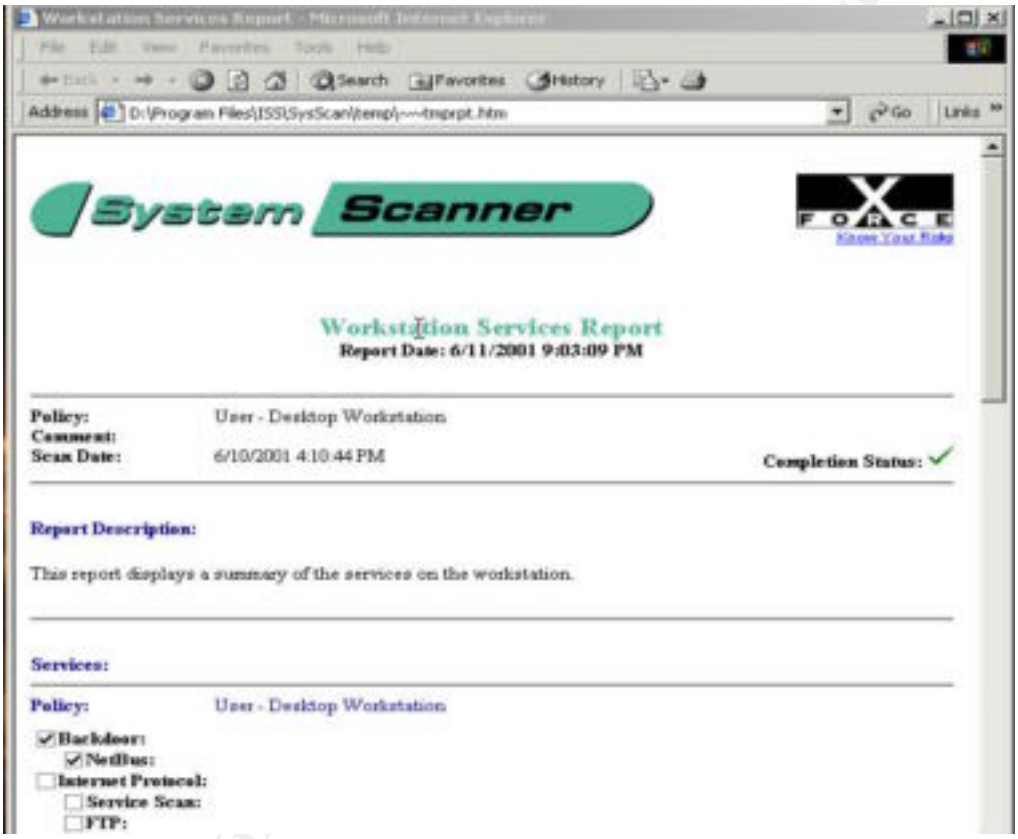

Figure 3.4.2-1 Sample Services Report

3.4.3 Trends Report

This report shows the history changes between two (2) scan results.

To view the Trends Report:

- From **Reports** menu, choose **Trends**.
- Select one (1) or more scans from the list. Hold down the **CRTL** key and click on the scans desired.
- Click **Next**.

- Click on **View the report in your web browser**.
- Click **Finish**.

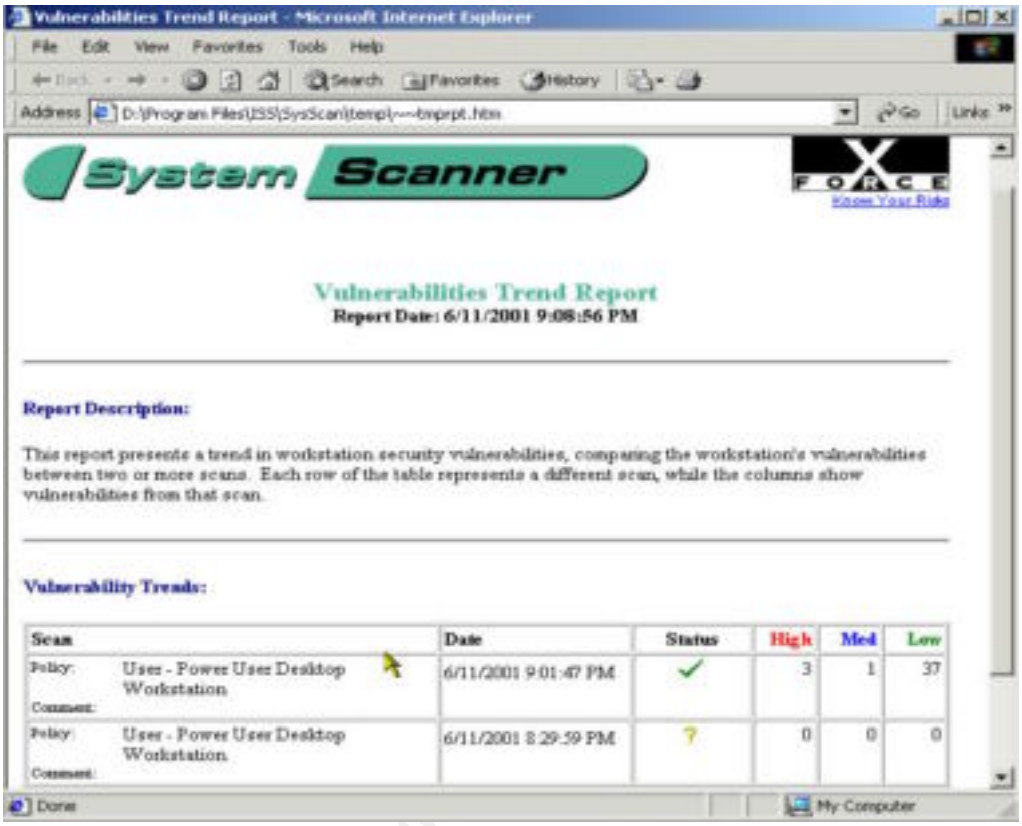

Figure 3.4.3-1 Sample Trends Report

3.4.4 Differential Report

This report shows the difference in vulnerabilities between two (2) scans. In this report the system administrator can choose whether or not to see the vulnerabilities in the first scan only, vulnerabilities in the second scan only, or the vulnerabilities that are common to both.

To view the Differential Report:

- From **Reports** menu, choose **Differential**.
- Under **Scans**, select the two (2) scans desired by holding down the **CTRL** key and clicking on the scans.
- Enable the appropriate option
  - **Vulnerabilities in 1st scan only**
  - **Vulnerabilities in 2nd scan only**
  - **Vulnerabilities common to both**
- Click **Next**

- Click on **View the report in your web browser**.
- Click **Finish**.

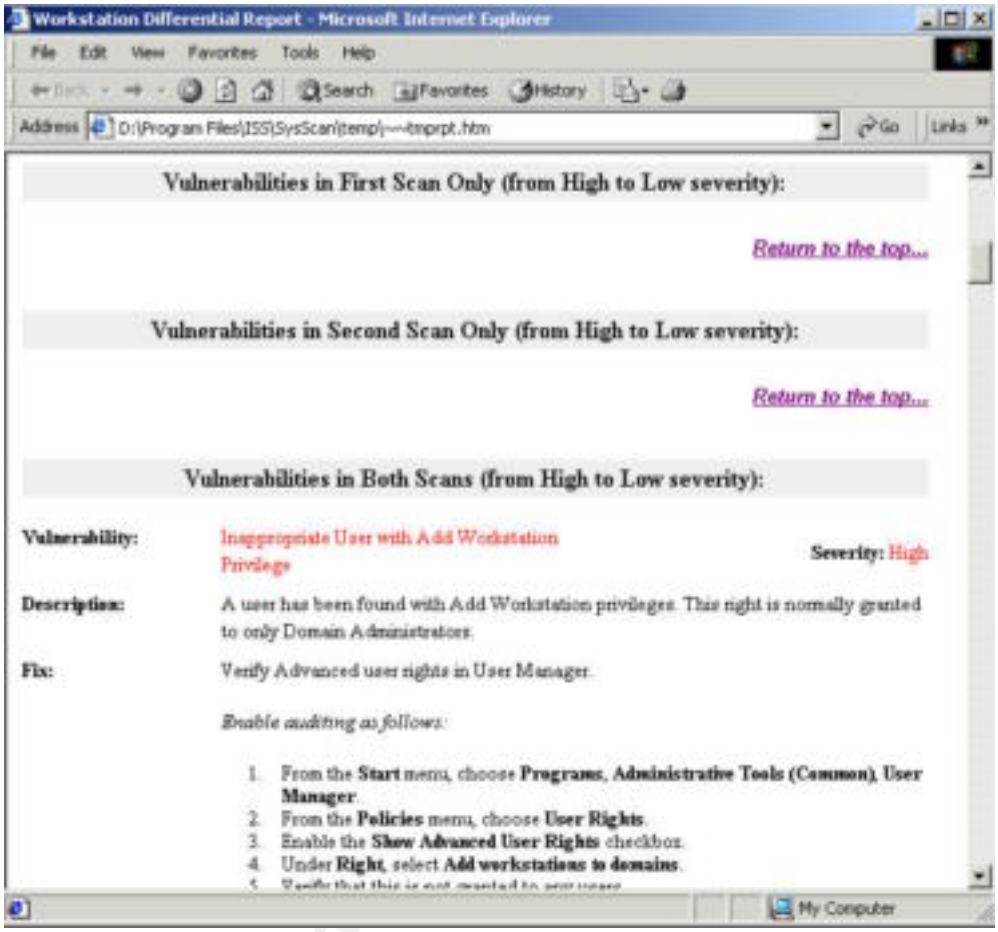

Figure 3.4.4-1 Sample Differential Report

3.5 Scheduled Scans

Schedule scans can be initiated to automatically scan the system and create vulnerability reports on a regular basis to make sure the system is always secure. These scans can be run with little or no supervision. The need for periodic scanning is based on the system's level of exposure to the Internet, the type and value of information on the system, and the frequency in which software is changed on the system.

There are several options to choose when scheduling a scan.

- Description
- Policy to use
- Frequency of scan (daily, weekly, monthly)

- Time of scan
- Day in which scan is to be run

3.5.1 How to Schedule a Scan

- From the **Setting** menu, choose **Schedule** – this will open up a dialog box for the schedule.
- Click **NEW**.
- Put in your description for the scan
- Select which policy to use for the scan
- Set the time, frequency and day for the scan
- Click **OK**.

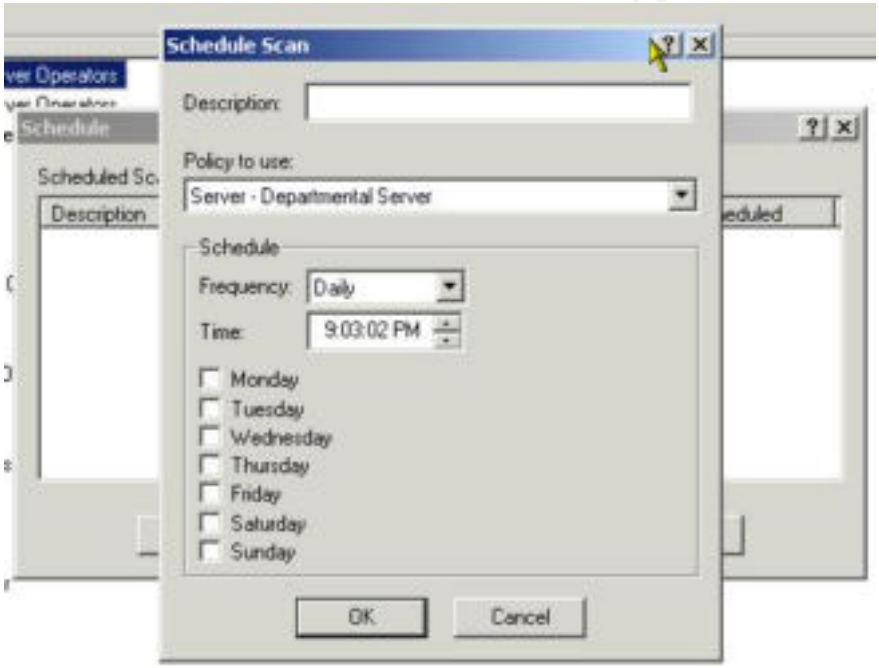

Figure 3.5.1-1 Scan Scheduling

The ability to modify and delete already existing scans to meet the needs of the system is provided in this option of the software.

3.5.2 Running a Scan in Background Mode

Scans can be run at system startup. To set System Scanner 1.1 to run automatically, follow the following steps:

- Click on **Settings, General, Basic**
- Click **Run a scan at low priority in background**.
- Select the policy to use

- Click **OK**.

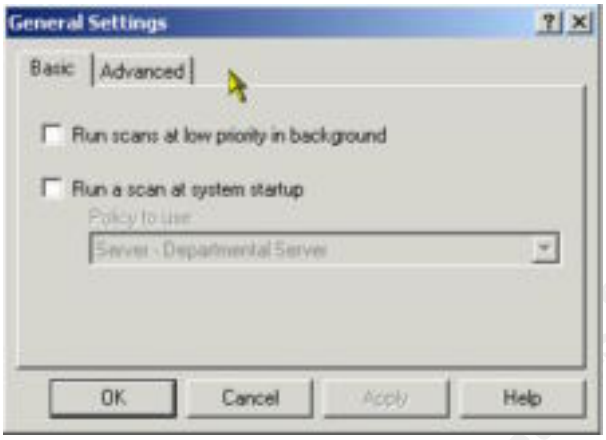

Figure 3.5.2-1 Background Mode Scan

4. SECURITY PRACTICES

ISS System Scanner 1.1 uses the Adaptive Security Model that provides real-time monitoring, detection, and response to vulnerabilities and intrusion.

This ideology is composed of four (4) integrated ISS approaches. First to be implemented is frequent automatic network scanning. Second is the response to security weaknesses for immediate correction. Third is the real-time intrusion detection that occurs around the clock for both internal and external attacks. And fourth, self-correction in response to security threats is automatic and dynamic.

There is no single "silver bullet" able to bring about a zero (0) risk to the system or network, though that would be the ideal method of securing the system. ISS System Scanner 1.1 is one of many tools that can be used to increase the security of a system.

In order for you to know what is going on with the system, there must be established security practices, which include monitoring, detection, and response. Running the System Scanner 1.1 schedule option on a system at regular intervals allows the system administrator the ability to maintain good security on the system.

5. FEATURES AND BENEFITS

Some of the key features of this software are:

- It will detect high-risk activity such as "back door" remote access programs like Back Orifice or users dialing into the system with a modem.

- It has a comprehensive set of security-related checks including over 300 MS Windows' specific security issues.

- It provides system "lock-down" capability, which can pinpoint unauthorized changes to system configuration.

- It will enforce change control policies.

- Provides automated policy compliance testing with vulnerability fix information.

- Gives rapid implementation of security policy.

System Scanner 1.1 offers a policy-oriented, straightforward methodology that protects data availability, integrity and confidentially. This methodology simplifies creating system security baselines for users, groups, shares, critical file systems and services. Once you have all your baseline metrics in place, this software locks down the host via digital fingerprinting to ensure the identification of systems that are being altered without permission. This process ensures that remedial action can perform easily and quickly. System Scanner 1.1 helps defend against insiders, the primary source of intrusions.

A comparison was run between System Scanner 1.1 on the local system and a licensed version of ISS System Scanner 4.0. The results between the two scans were quite significant. System Scanner 1.1 revealed more vulnerabilities on the system than the licensed network version, System Scanner 4.0. The local scan showed three (3) high, twenty-one (21) medium and more that eighty (80) low vulnerabilities. The network scan only showed one (1) medium and three (3) low vulnerabilities. Since the software is loaded directly on the local system, it has registry and file permissions that the network version is not allowed. Therefore, the local software had the ability to check for more vulnerabilities. Since System Scanner 1.1 revealed more vulnerabilities that the licensed network version, it would benefit the system administrator to have the software loaded locally.

If there are applications installed on the system under test, such as MS Office, System Scanner 1.1 will report the application that exposes the system to a large number of DCOM objects that can be used with scripting languages and may enable an attacker to subvert the system. It is up to the judgment of the system administrator of each system to determine which may or may not be an acceptable risk. System Scanner 1.1 provides a tool to identify potential risks for the system administrator.

6. POTENTIAL DRAWBACKS AND SHORTCOMINGS

The unlicensed product has a lack of central management capabilities, plus a few reporting deficiencies. The licensed version is reported to have a better central management capability than the unlicensed product. In order for the unlicensed version to continue to be a useful security tool, there would need to be a method by

which updates to the software would be available on a timely basis. As software revisions are installed and additional vulnerabilities are identified, System Scanner must have corresponding updates, much like the anti-virus ".dat" files. The System Scanner 1.1 file on the Windows 2000 Resource Kit CD is dated 8/23/99, so vulnerabilities identified since that date cannot be located using this revision.

7. CONCLUSION

In order for systems to be as clean as possible from vulnerabilities, periodic scans should be performed on the systems. Though no networked system will never be 100% free from hostile attacks, the ability to know when and if your system becomes a target is easier. System Scanner 1.1 provides the system administrator with the tool to perform periodic checks on the system, and by customizing the scan policies, the ability to nail down the system as secure as possible. Some of the ways this product can help do this is using the auto-scheduler to routinely run scans without intervention and provide a method for fixing vulnerabilities found on the system. Because custom policies can be created, System Scanner 1.1 can be tailored for a wide range of system intrusions and threats.

8. REFERENCES

Phillips, Ken, ISS Scanner Guards the Weakest PC Link, PCWEEK, January 1999

Bennett, Jonathan, First Look: Network Edition, PC MAGAZINE

ISS System Scanner 1.1 Help Files

"Read Me" File from the Windows 2000 Resource Kit Security Tools

Smith, Randy Franklin, Top 10 Security Tools in the W2K Server Resource Kit, Windows 2000 Magazine, December 2000

9. ACRONYMS

DCOM	Distributed Component Object Model
DMZ	Demilitarized Zone
DoS	Denial of Service

FTP	File Transfer Protocol
ISS	Internet Security System
MB	Megabyte
MS	Microsoft
NTFS	NT File System
OS	Operating System
RAM	Random Access Memory
RAS	Remote Access Server
TCP/IP	Transfer Control Protocol / Internet Protocol