

Glossary

A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z

A

[attack signatures](#)

B

[baseline database](#)

[baseline scan](#)

[brute force vulnerabilities](#)

C

[CERT](#)

[check](#)

[communications protocol](#)

[cookie](#)

[cryptography](#)
[custom scan](#)
[ciphertext](#)

D

[data segments](#)
[default policy \(Server-DMZ FTP or Mail Server\)](#)
[default policy \(Server-DMZ Web Server\)](#)
[default policy \(Server – Intranet Server\)](#)
[default policy \(Server – Departmental NT Server\)](#)
[default policy \(User – Power User NT Desktop\)](#)
[default policy \(User – NT Desktop Workstation\)](#)
[default policy \(Technical – Baselines\)](#)
[default policy \(Technical – Browser Only\)](#)
[default policy \(Technical – Heavy Scan\)](#)
[default policy \(Technical – NT OS Lockdown\)](#)
[default policy \(Technical – Services Scan\)](#)
[denial of service \(DoS\) vulnerabilities](#)
[dialog](#)
[Differential Reports](#)
[DLL](#)
[Dynamic Software](#)

E

[exploit](#)

F

[file Baseline](#)
[fix](#)
[FTP](#)

G

[GUI](#)
[group scan baseline](#)

H

[header](#)
[host](#)
[HTML](#)

I

[Internet Explorer vulnerabilities](#)
[IP \(Internet Protocol\) address](#)
[IP spoofing vulnerabilities](#)

J

[Java](#)

K

L

M

[micro-update](#)

N

[NetBIOS](#)

[Netscape Navigator vulnerabilities](#)

O

P

[patch](#)

[plaintext](#)

[policy](#)

[Policy Editor](#)

[process baseline](#)

[progress bar](#)

[protocol](#)

[purge duration](#)

Q

R

[regedit.exe](#)

[regedt32.exe](#)

[registry scan baseline](#)

[registry](#)

[registry key](#)

[report](#)

[RFC](#)

[risk level](#)

S

[scans results database](#)

[scan](#)

[Server - Departmental Server](#)

[Server-DMZ FTP or Mail Server](#)

[Server-DMZ Web Server](#)

[Server - Intranet Server](#)

[services baseline](#)

[services report](#)

[share scan baseline](#)

[spooof](#)

[SSCLI](#)

[SSCLI parameters](#)

[system](#)

[system requirements](#)

T

[TCP/IP](#)

[Technical - Baselines](#)

[Technical - Browser Only](#)

[Technical - Heavy Scan](#)

[Technical - NT OS Lockdown](#)

[Technical - Services Scan](#)

[trends report](#)

[trojan horse](#)

U

[URL](#)

[User Manager](#)

[User - Desktop Workstation](#)

[User - Power User Desktop Workstation](#)

[User - Home Computer](#)

[baseline](#)

V

[virus](#)

[vulnerability](#)

[vulnerability database](#)

[vulnerabilities report](#)

W

[WEB server](#)

[window](#)

[Windows NT auditing/miscellaneous vulnerabilities](#)

[Windows NT registry vulnerabilities](#)

[Windows NT users vulnerabilities](#)

[wizard](#)

X

Y

[Y2K](#)

Z

Scan

A scan runs [policies](#) which perform [checks](#) that detect weaknesses and vulnerabilities on your system.

Vulnerability

A vulnerability is a security hole in a system which could allow an intruder to gain information and lead to improper access.

Micro-Update

A micro-update is a periodical software update between major software releases. A micro-update consists of the most recently developed [checks](#) that detect the latest vulnerabilities on your system. The online help system is automatically updated during a micro-update.

Fix

A fix is information provided for correcting vulnerabilities found during a scan.

Host

A host is a computer with an [IP address](#).

Wizard

A wizard is a program that guides you through a procedure. System Scanner uses policy Wizards for creating, editing, and copying [policies](#).

DLL

A dll is a dynamic link library file type. System Scanner uses DLLs to accomplish [micro-updates](#).

Denial of Service (DoS)

A denial of service (DoS) is an attack in which an intruder severely limits or crashes your system by sending an abundance of packets containing oversized [data segments](#) , incorrect [header](#) information, and overloaded service requests.

Exploit

An exploit is a method that tries to find vulnerabilities by running hacker subroutines on your system. System Scanner may run exploits on your system during a [scan](#).

Dialog

A dialog is a viewing area on your screen that is not scalable. System Scanner uses rectangular dialogs.

Report

A report provides you with rapid, formatted summaries of [vulnerabilities](#) detected on your system. System Scanner provides the ability to generate [HTML](#) -based activity reports that are used for security assessment of your system. System Scanner provides three types of reports: [vulnerabilities report](#) , [services report](#) , and [trends report](#).

Attack Signature

An attack signature is a recognized pattern of activity that could be used to exploit weaknesses in a given machine or network. System Scanner provides [checks](#) for attack signatures.

Progress Bar

A progress bar is a standard [GUI](#) component used to show the relative amount of a task that is completed and how much is left.

IP (Internet Protocol) Address

An IP address is the physical address of a computer attached to a TCP/IP network. Every computer on the network must have a unique IP address. IP addresses are four sets of numbers separated by periods; for example, 204.171.64.2.

Risk Level

Risk levels are used to show the risk of vulnerabilities found on your system during a scan. ISS classifies risk levels as follows:

Low - it provides access to network data that might be sensitive, but is less likely to lead to a higher-risk exploit.

Medium - it provides access to sensitive network data that might lead to higher-risk exploits.

High - it provides unauthorized access to the host or to the network. High Risk vulnerabilities should be corrected immediately.

System Requirements

You must satisfy System Scanner's system requirements before you can successfully install and run it on your machine. The system requirements below present all required and recommended features needed for System Scanner. Meeting the recommended requirements increases the performance and reliability of System Scanner.

Required

- 75 MHz Pentium
- 16 MB of RAM
- 20 MB of disk space for database entries
- Windows 95 or Windows NT 3.0

Recommended

- 133 MHz Pentium or better
- 32 MB of RAM or better
- 35 MB of disk space for database entries
- Windows 95 or Windows NT 4.0 w/ Service Pack 3

If your system meets these recommendations and not operating as expected, contact technical support tsupport@iss.net .

Services Report

Service reports show all services running on your system and what port they are running on. If this port is different than the recommended port numbers maintained by the Internet Assigned Numbers Authority (IANA) at <http://www.iana.org/>, it is a potential [vulnerability](#).

[More on reporting](#)

Trends Report

Trend reports show the history change between selected scan results in the [scan results database](#).

[More on reporting](#)

Vulnerabilities Report

This report shows all [vulnerabilities](#) found on your system along with step by step security assessment information.

[More on reporting](#)

Brute Force Vulnerabilities

This type of vulnerability allows an intruder to bombard your system with a flood of attempts to hack the system, generally by attempting to log in through any available service. It is based on the assumption that users will not change their passwords often, and that eventually the brute force attack will discover the password.

Windows NT Users Vulnerabilities

This type of vulnerability allows an intruder gains access to your system by retrieving Windows NT users accounts and passwords by checking for guessable passwords, missing passwords, password history, insecure policies, log off settings, and lockout settings.

Windows NT Registry Vulnerabilities

This type of vulnerability allows an intruder to remotely gain access to the registry of your Windows NT machine. This is done by checking for Windows NT Remote Access Service (RAS), Local Security Authority (LSA), auto logon, changeable [registry](#) file associations, DCOM permissions, IP forwarding, and various missing patches.

Windows NT Auditing/Miscellaneous Vulnerabilities

This type of vulnerability allows an intruder can gain access to your system by taking advantage of accessible event logs, readable repair directories, non-updated security patches, and various missing patches.

IP Spoofing Vulnerabilities

This type of vulnerability allows an intruder to [spoof](#) packets to your system by taking advantage of TCP sequence prediction, insecure sockets, and predictable passwords.

Netscape Navigator Vulnerabilities

This type of vulnerability allows an intruder to gain access to your system by taking advantage of weak Netscape Navigator settings, such as insecure form disabled, mixed disabled, [Java](#) enabled, JavaScript enabled, and [plaintext](#) disabled.

Internet Explorer Vulnerabilities

This type of vulnerability allows an intruder can gain access to your system by taking advantage of weak Internet Explorer settings such as low security enabled, [Java](#) enabled, send check disabled, view check disabled, [cookies](#) always accepted, bad certificate disabled, open post disabled, and more.

Scan Results Database

The scan results database stores all scan results. Scan results remain here until you [purge the database](#). You can use this database to generate reports for security assessment by generating [trend reports](#) and [differential reports](#).

CERT Coordination Center

The CERT* Coordination Center studies Internet security vulnerabilities, provides incident response services to sites that have been the victims of attack, publishes a variety of security alerts, researches security and survivability in wide-area-networked computing, and develops information to help you improve security at your site.

Baseline Scan

A baseline scan is run to familiarize System Scanner with all current configurations of your system. Any changes after the baseline scan are reported as [vulnerabilities](#).

[Generating the Baseline Database](#)

Policy

A policy is a group of [checks](#) that are run during a scan. You can create a policy manually or System Scanner can automatically create a policy based on the needs of your system.

NOTE: A policy is required for scanning.

Custom Scan

A custom scan is running any [policy](#) that does not use a default policy.

Vulnerability Database

The vulnerability database contains current [checks](#) needed for security assessment. [Micro-updates](#) ensure that this database is current.

System

System refers to the machine in which System Scanner is installed.

Purge Duration

The purge duration is the number of days the scan results exist in the [scan_results database](#) between purging.
Purging the Scan Results Database

Trojan Horse

A trojan horse is a program that appears legitimate, but performs some illicit activity when it is run. It may be used to locate password information or make the system more vulnerable to future entry or simply destroy programs or data on the hard disk.

Virus

A virus is software that “infects” your system and buries itself into an existing program. Once that program is executed, the virus code is activated and attaches copies of itself to other programs in the system. Infected programs copy the [virus](#) to other programs and so on.

URL

A URL (Uniform Resource Locator) is an address that defines the location to a file on the Web or any other Internet facility. For example, <http://www.iss.net>.

RFC

An RFC (Request for Comment) is a published document that describes the specifications for a recommended technology. RFCs are used by the Internet Engineering Task Force (IETF) and other standards bodies. RFCs are available from many sources including http://www.yahoo.com/Computers_and_Internet/Standards/RFCs/.

Checks

Checks are located in the [GUI](#) and used when creating or modifying policies to run scans on your system.

Regdt32

Regedt32 is the [registry editor](#) for Windows NT.

Baseline Database

The baseline database is the key component used to monitor changes in your system. System Scanner uses the baseline, during a [baseline scan](#), to report if an intruder has gained access to your system and modified the files or registry keys.

HTML

HTML (HyperText Markup Language) is the document format used on the World Wide Web. Web pages are built with HTML tags, or codes, embedded in the text. HTML defines the page layout, fonts and graphic elements as well as the hypertext links to other documents on the Web.

GUI

A GUI (Graphical User Interface) is the graphics-based user interface that incorporates icons, pull-down menus and a mouse pointer. The GUI is the standard way users interact with a computer.

Data Segments

Data segments are reserved areas or pieces of a larger data structure within a [communications protocol](#).

Communications Protocol

A communications protocol is a set of rules that govern the operations of functional units to achieve communication. (e.g., [TCP/IP](#))

TCP/IP

(Transmission Control Protocol/Internet Protocol) is a [communications protocol](#) of the Internet and supports most computer environments.

Header

The header is the first part in a [communications protocol](#) which contains controlling data, such as originating and destination stations, message type and priority.

Differential Reports

Differential reports show the differences of [vulnerabilities](#) found between two scans. The differential options are as follows:

- [Vulnerabilities in 1st scan only](#)
- [Vulnerabilities in 2nd Scan Only](#)
- [Vulnerabilities Common to Both](#)

[More on reporting](#)

File Scan Baseline

The file scan baseline is a "snap shot" of the file configuration on your system. It is used to determine file changes that occur on your system. If these changes are not authorized or known by a trusted user, they are considered [vulnerabilities](#).

Group Scan Baseline

The group scan baseline is a "snap shot" of the group settings on your system. These settings include group rights and users. The Group scan baseline is used to determine the group changes that occur on your system. If these changes are not authorized or known by a trusted user, they are considered [vulnerabilities](#).

Registry Baseline

The registry baseline is a "snap shot" of the registry configuration on your system. It is used to determine registry key changes that occur. If these changes are not authorized or known by a trusted user, they are considered [vulnerabilities](#).

Registry Key

Registry keys are used to determine the hardware and environment of your system. They are created/modified when you add or remove software/hardware.

Registry

The registry consists of [registry keys](#) , and is used to control the hardware and environment of your system. The Windows NT registry is accessed via regedt32.exe and the Windows 95 registry is accessed via regedit.exe.

Cookie

A cookie is a chunk of data created by a [Web server](#) that is stored on your system. It provides a way for the Web site to keep track of a your patterns and preferences and, with the cooperation of the Web browser, to store them on the your own hard disk.

Java

A programming language for Internet (World Wide Web) and intranet applications. Java programs are called from HTML documents or launched as stand alone programs.

Plaintext

Plaintext is readable text that is not encrypted. See [cryptography](#).

Cryptography

Cryptography is the conversion of data into a secret code for secure transmission. [Plaintext](#) is converted into a coded equivalent called [ciphertext](#) via an encryption algorithm. The ciphertext is decoded (decrypted) at the receiving end and turned back into plaintext for readability.

Ciphertext

Ciphertext is data that is unreadable in its current form. Ciphertext is created during [cryptography](#) and is used for secure data transmission.

WEB Server

A WEB server is a computer that provides World Wide Web services on the Internet.

Share Scan Baseline

The share scan baseline is a "snap shot" of your system's share settings. The settings include hidden shares, share permissions on an NTFS directory, permissions on the share itself, and printer share permissions. The share scan baseline is used to determine the share changes that occur on your system. If these changes are not authorized or known by a trusted user, they are considered [vulnerabilities](#).

User Scan Baseline

The user scan baseline is a "snap shot" of your system's user settings. The settings include logon settings, RAS settings, and user rights. The user scan baseline is used to determine the share changes that occur on your system. If these changes are not authorized or known by a trusted user, they are considered [vulnerabilities](#).

Services Baseline

The service baseline is a "snap shot" of your system's service and device settings. The settings include service applets and device applets. The service baseline is used to determine the share changes that occur on your system. If these changes are not authorized or known by a trusted user, they are considered [vulnerabilities](#).

FTP

FTP (File Transfer Protocol) is a protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). It includes functions to log onto the network, list directories and copy files. It can also convert between the ASCII and EBCDIC character codes. FTP operations can be performed by typing commands at a command prompt or via an FTP utility running under a graphical interface such as Windows. FTP transfers can also be initiated from within a Web browser by entering the URL preceded with ftp://.

Process Baseline

The process baseline is a "snap shot" of your system's startup programs. The process baseline reports changes to the common Run key in registry, common Startup folder, load and run values (specify programs that are auto-started), user specific Run key in registry, and user specific Startup folder. If these changes are not authorized or known by a trusted user, they are considered [vulnerabilities](#).

Window

A window is a scalable viewing area on your screen. System Scanner uses rectangular windows.

Regedit.exe

Regedit.exe is the [registry editor](#) for Windows 95.

Dynamic Software

Dynamic software is software that is installed, uninstalled, or upgraded frequently. Hence, any software that causes the [registry keys](#) to change must be added to the baseline and your system should be scanned using a [baseline policy](#).

Spoof

Faking the sending address of a transmission in order to gain illegal entry into a system.

Protocol

Different from communications protocol. A protocol is a set of rules used to facilitate communications.

Registry Editor

The registry editor is software used to change the [registry](#) . See [regedt32.exe](#) and [regedit.exe](#) .

NetBIOS

A commonly-used network protocol for PC local area networks. NetBIOS provides session and transport services (layers 4 and 5 of the OSI model). NetBIOS did not provide a standard frame format for transmission over the network, causing various different implementations of NetBIOS to be created. For example, Artisoft's LANtastic uses a proprietary version of NetBIOS for transmission between client and server. The frame format was later formalized in NetBEUI, which is used in all Windows operating systems that support networking.

There are two NetBIOS modes. The Datagram mode is the fastest mode, but does not guarantee delivery. It uses a self-contained packet with send and receive name, usually limited to 512 bytes. If the recipient device is not listening for messages, the datagram is lost. The Session mode establishes a connection until broken. It guarantees delivery of messages up to 64KB long.

Y2K

Y2K (Year 2000) refers to the year 2000 date bug in all computers that are not patched. Any un-patched computers are threatened by the limited date integers. In the year 2000, the dates will be reset which could possibly lead to catastrophic results.

Patch

Patches are executable programs provided by manufacturers that repair bugs or potential security weaknesses in software. System Scanner requires you to apply patches to correct patch-related vulnerabilities.

User Manager

User Manager is a software tool you can use to manage security for a computer running Windows NT Workstation. It is used to Manage the users and groups of your network.

Policy Editor

The Policy Editor is Windows 95 and Windows 98 software used to create and manage policies for a user or group of users on a network.

NOTE: The policy editor is **not** installed by default. You must install it from ADMIN\APPTOOLS\POLEDIT on the Windows CD.

System Scanner Command Line (SSCLI)

The SSCLI allows you to access the System Scanner Agent via command line [parameters](#). This is useful when using SMS push commands to multiple systems on a network.

SSCLI Parameters

The SSCLI parameters are defined below.

Parameter	Operation
-noscan	Don't run a scan (e.g., user may just want to run a report).
-sched	Designed to be used after a new schedule has been downloaded, this simply tells SSCLI to launch SysScan Agent and immediately exit. SysScan Agent always checks for scheduled items on startup. This option has no effect if a scan is to be run (since SysScan Agent will be loaded anyway in order to do the scan).
-us	On exit, unload SysScan Agent even if scheduled items exist.
-uf	On exit, force an unload of SysScan Agent (no matter what).
-p	Specifies name of policy to use (if a scan is to be run).
-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). Note that these are simply the hotkeys found in the System Scanner Report Wizard's UI for the corresponding report options.

Server-DMZ FTP or Mail Server Policy

Any NT server system that is installed in a DMZ that does **not** run a web server. Due to the heavily exposed nature of the system (easily subject to attack), all checks except for IIS, browser, MS office, and modem checks are enabled.

Server-DMZ Web Server Policy

Any NT server system that is installed in a DMZ that runs a web server. Due to the heavily exposed nature of the system (easily subject to attack), all checks except for browser, MS office, and modem checks are enabled.

Server - Intranet Server Policy

Internal (typically web) servers. Since these systems are installed behind firewalls, they are less exposed to attack. As a result, fewer checks are enabled than for DMZ systems. Specifically, Denial of Service or virus scanner checks are not enabled.

Server - Departmental Server Policy

These systems are typically less critical than Intranet servers, in that disruptions are confined to particular departments, rather than the entire organization. Fewer checks are offered than for Intranet servers. Specifically, Registry, NetBios, and IIS checks are not enabled.

Technical – Baselines Policy

Only MD5 baselines are enabled, to test system configuration lock down.

User - Power User Desktop Workstation Policy

These systems are used by computer savvy individuals who prefer to have a more robust system and are willing to spend a little effort tweaking their system configuration.

User - Desktop Workstation Policy

This is the typical Windows user desktop workstation. Only issues that could compromise the entire organization are enabled.

Technical - Browser Only Policy

Only web browser software settings are checked.

Technical - Heavy Scan Policy

All checks are enabled.

Technical - OS Lockdown Policy

Most baseline checks are enabled.

Technical - Services Scan Policy

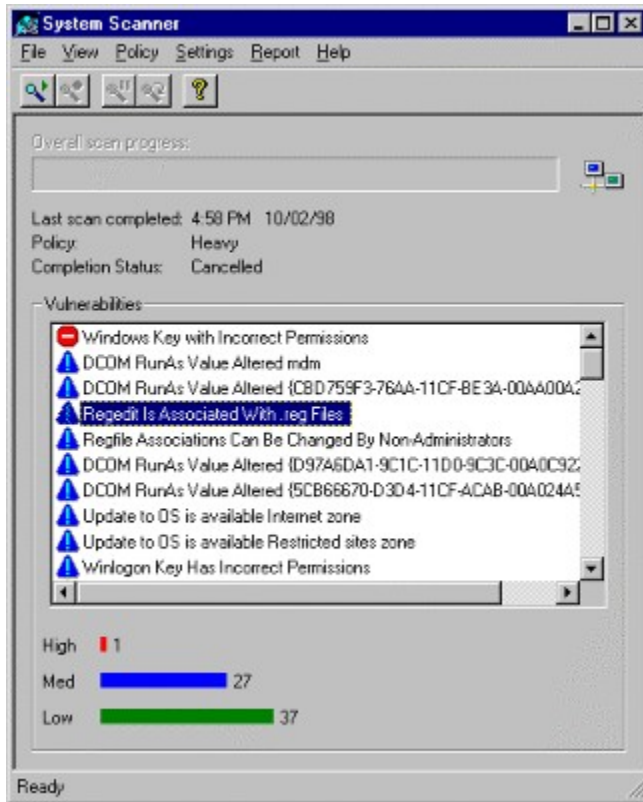
Checks that audit server applications that might be running are enabled.

User - Home Computer

Checks that scan for viruses, backdoors, or software settings that can hinder the performance and/or reliability of your system.

Main window


How Do I Open This?



New Policy Wizard

How Do I Open This?

New Policy Wizard



This wizard helps you create a new policy that can then be used when scanning your computer for security vulnerabilities.

Name of new policy:

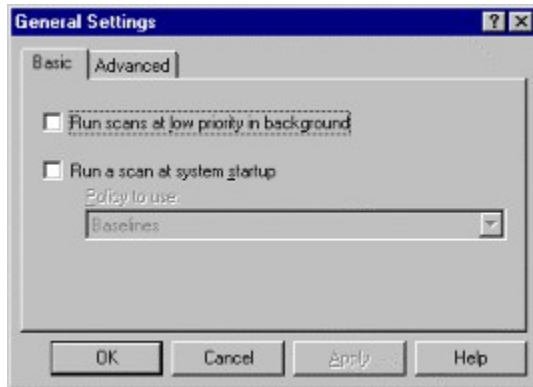
I want the wizard to:

- Suggest settings for me
- Let me choose all settings for myself

< Back Next > Cancel Help

General Settings Dialog (Basic)

How Do I Open This?

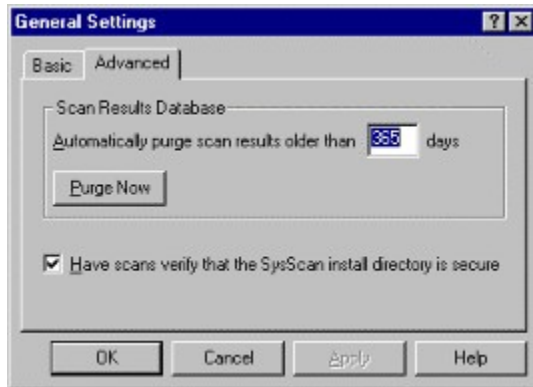


How do I open this?

1. Double click on the Tray Icon. This will open the main window.
2. From the **Settings** menu, Choose **General**.

General Settings Dialog (Advanced)

How Do I Open This?



Dialog Index

[Main window](#)

[General Settings Dialog \(Basic\)](#)

[General Settings Dialog \(Advanced\)](#)

[Vulnerabilities Report Dialog](#)

[Services Report Dialog](#)

[Trends Report Dialog](#)

[Trends Report Dialog](#)

[Differential Reports Dialog](#)

[Schedule Dialog](#)

[Tray Icon](#)

[New Policy Wizard](#)

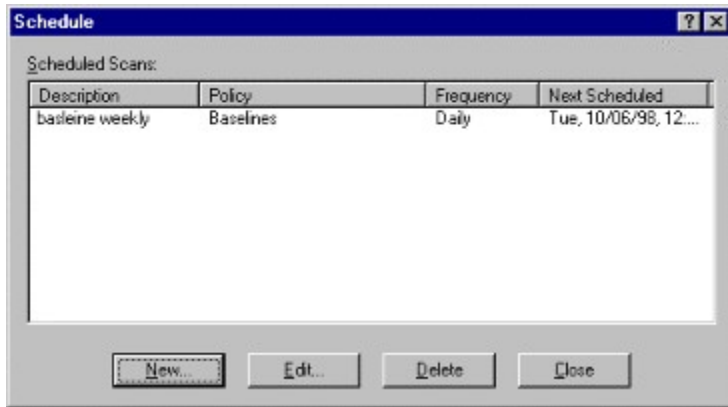
[Copy and Edit Policy Wizard](#)

[Delete Policy](#)

[Rename Policy](#)

Schedule Dialog

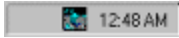
How Do I Open This?



Tray Icon

System Scanner will always display an icon in the Windows system tray whenever it is running. Double clicking the icon brings up the UI and the following menu items are displayed with a right mouse click.

- Show (UI)
- Scan Now
- Stop Scan
- Pause Scan
- Close
- Close and Exit (if administrator allows it)



How do I open this?

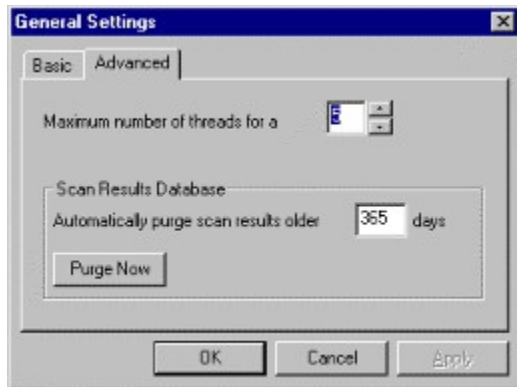
- 1. Double click** on the **tray icon**.

How do I open this?

1. **Double click** on the **tray icon**. This will open the **main window**.
2. From the **Policy** menu, choose **New**.

General Settings Dialog (Advanced)

How Do I Open This?

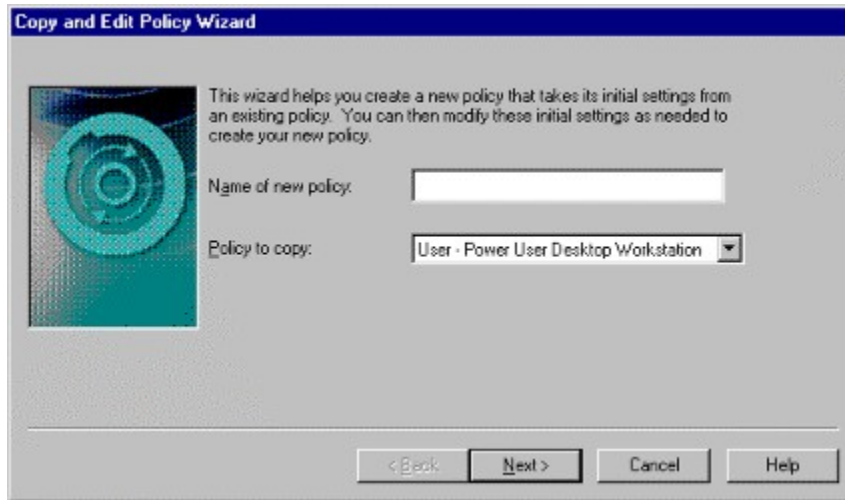


How do I open this?

1. **Double click** on the **tray icon**. This will open the **main window**.
2. From the **Settings** menu, choose **General**.
3. **Click** on the **Advanced** tab.

Copy and Edit Policy Wizard

How Do I Open This?



The screenshot shows a dialog box titled "Copy and Edit Policy Wizard". On the left is a circular graphic with a blue and green gradient. To the right of the graphic is the following text: "This wizard helps you create a new policy that takes its initial settings from an existing policy. You can then modify these initial settings as needed to create your new policy." Below this text are two input fields: "Name of new policy:" followed by an empty text box, and "Policy to copy:" followed by a dropdown menu showing "User - Power User Desktop Workstation". At the bottom of the dialog are four buttons: "< Back", "Next >", "Cancel", and "Help".

Copy and Edit Policy Wizard

This wizard helps you create a new policy that takes its initial settings from an existing policy. You can then modify these initial settings as needed to create your new policy.

Name of new policy:

Policy to copy:

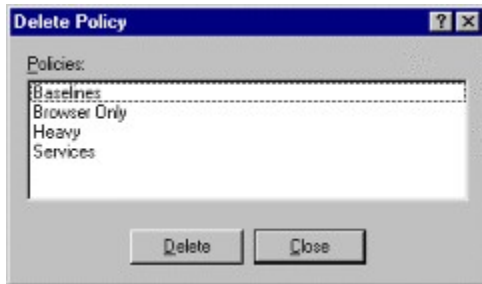
< Back Next > Cancel Help

How do I open this?

1. **Double click** on the **tray icon**. This will open the **main window**.
2. From the **Policy** menu, choose **Copy and Edit**.

Delete Policy

[How Do I Open This?](#)

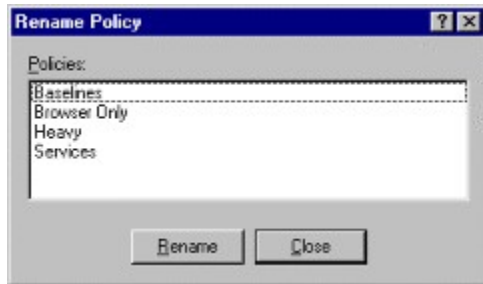


How do I open this?

1. **Double click** on the **tray icon**. This will open the **main window**.
2. From the **Policy** menu, choose **Delete**.

Rename Policy

[How Do I Open This?](#)



How do I open this?

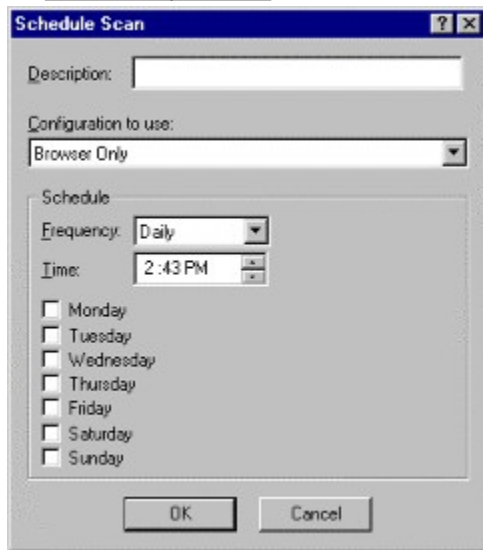
1. **Double click** on the **tray icon**. This will open the **main window**.
2. From the **Policy** menu, choose **Delete**.

How Do I Open This?

- 1. Double click** on the **tray icon**. This will open the **main window**.
- From the **Settings** menu, choose **Schedule**.

Schedule Configuration Dialog

How Do I Open This?



The image shows a Windows-style dialog box titled "Schedule Scan". It contains the following elements:

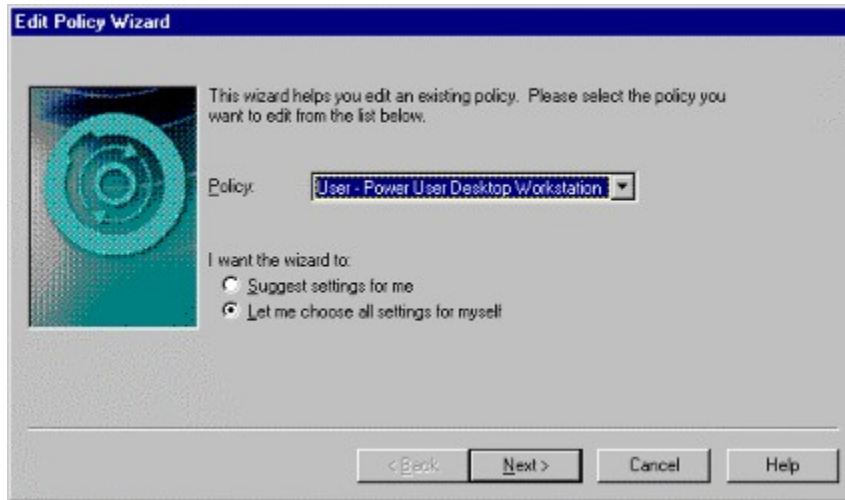
- Description:** A text input field.
- Configuration to use:** A dropdown menu currently showing "Browser Only".
- Schedule:** A section containing:
 - Frequency:** A dropdown menu set to "Daily".
 - Time:** A time selection control set to "2:43 PM".
 - A list of days of the week, each with an unchecked checkbox:
 - Monday
 - Tuesday
 - Wednesday
 - Thursday
 - Friday
 - Saturday
 - Sunday
- Buttons:** "OK" and "Cancel" buttons at the bottom.

How Do I Open This?

- 1. Double click** on the **tray icon**. This will open the **main window**.
- From the **Settings** menu, choose **Schedule**.
- Click **New**.

Edit Policy Wizard

How Do I Open This?



The screenshot shows the 'Edit Policy Wizard' dialog box. It has a blue title bar and a grey background. On the left, there is a circular graphic with a blue and green gradient. To the right of the graphic, the text reads: 'This wizard helps you edit an existing policy. Please select the policy you want to edit from the list below.' Below this text is a 'Policy:' label followed by a dropdown menu showing 'User - Power User Desktop Workstation'. Underneath the dropdown, the text says 'I want the wizard to:' followed by two radio button options: 'Suggest settings for me' (which is unselected) and 'Let me choose all settings for myself' (which is selected). At the bottom of the dialog, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Edit Policy Wizard

This wizard helps you edit an existing policy. Please select the policy you want to edit from the list below.

Policy: **User - Power User Desktop Workstation**

I want the wizard to:

- Suggest settings for me
- Let me choose all settings for myself

< Back Next > Cancel Help

How Do I Open This?

1. **Double click** on the **Tray Icon**. This will open the **Main window**.
2. From the **Policy** menu, choose **Edit**.

Vulnerabilities Report Dialog

[How Do I Open This?](#)

Vulnerabilities Report

Scans:

Date	Policy	Comment
✓ 10/05/98 00:39...	test	
10/05/98 00:39...	Baselines	
10/02/98 16:58...	Heavy	
10/02/98 16:57...	Heavy	
10/02/98 16:55...	Heavy	
10/02/98 16:50...	Heavy	
✓ 10/02/98 14:03...	Heavy	
10/02/98 14:03...	Heavy	

Vulnerability Severity

- High Risk
- Medium Risk
- Low Risk

Report Detail

- Full Description
- Fix Information
- Scan Policy Info

Differential

Show vulnerabilities:

- In 1st Scan Only
- In 2nd Scan Only
- Common to Both

< Back Next > Cancel Help

How Do I Open This?

- 1. Double click** on the **Tray Icon**. This will open the **Main window**.
- From the **Report** menu, choose **Vulnerabilities**.

Services Report Dialog

[How Do I Open This?](#)

Services Report

Scans:

Date	Policy	Comment
✓ 10/05/98 00:39...	test	
10/05/98 00:39...	Baselines	
10/02/98 16:58...	Heavy	
10/02/98 16:57...	Heavy	
10/02/98 16:55...	Heavy	
10/02/98 16:50...	Heavy	
✓ 10/02/98 14:03...	Heavy	
10/02/98 14:03...	Heavy	

Vulnerability Severity

- High Risk
- Medium Risk
- Low Risk

Report Detail

- Full Description
- Exp Information
- Scan Policy Info

Differential

Show vulnerabilities:

- In 1st Scan Only
- In 2nd Scan Only
- Common to Both

< Back Next > Cancel Help

How Do I Open This?

- 1. Double click** on the **tray icon**. This will open the **Main window**.
- From the **Report** menu, choose **Services**.

Trends Report Dialog

[How Do I Open This?](#)

Trends Report

Scans:

Date	Policy	Comment
✓ 10/05/98 00:39...	test	
10/05/98 00:39...	Baselines	
10/02/98 16:58...	Heavy	
10/02/98 16:57...	Heavy	
10/02/98 16:55...	Heavy	
10/02/98 16:50...	Heavy	
✓ 10/02/98 14:03...	Heavy	
10/02/98 14:03...	Heavy	

Vulnerability Severity

- High Risk
- Medium Risk
- Low Risk

Report Detail

- Full Description
- Exp Information
- Scan Policy Info

Differential

Show vulnerabilities:

- In 1st Scan Only
- In 2nd Scan Only
- Common to Both

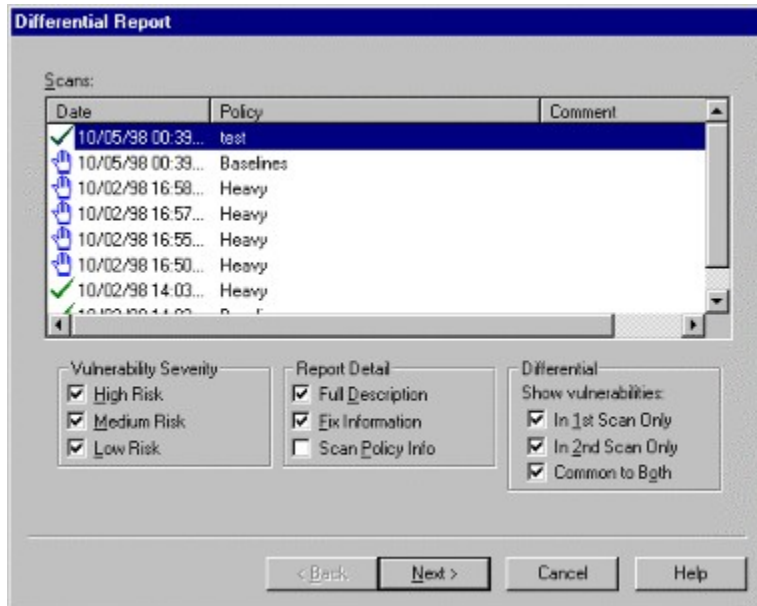
< Back Next > Cancel Help

How Do I Open This?

1. **Double click** on the **tray icon**. This will open the **main window**.
2. From the **Report** menu, choose **Trends**.

Differential Reports Dialog

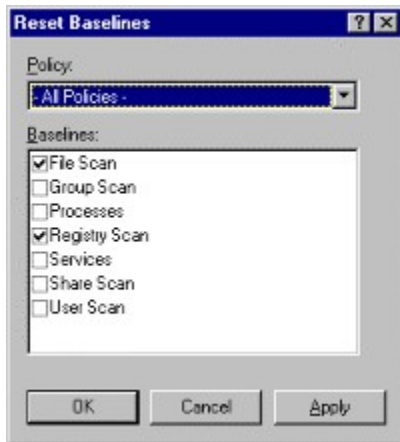
How Do I Open This?



How Do I Open This?

1. **Double click** on the **tray icon**. This will open the **main window**.
2. From the **Report** menu, choose **Differential**.

Reset Baseline Dialog



All Access NetBIOS Share - Everyone

A NetBIOS share has been found with no access control. This allows anyone full access to any resources provided, and can also allow access to the entire hard drive on unpatched versions of Windows 95.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Correct the share permissions or remove the share.

Set the permissions explicitly as follows:

1. Navigate to the share in Windows Explorer.
2. Right-click the share, select **Properties**.
3. Under the **Sharing** tab, review the permissions.
4. Allow access only to approved users.
5. Click **OK**.

-OR-

Open the command line, remove the share as follows:

1. From the **Start** menu, select **Run**.
2. Type **cmd**, then click **OK**. This opens the command line.
3. Type **net share sharename /delete**, where sharename is the name of the share.
4. Type **exit** to return to the Windows NT desktop.

All Access NetBIOS Share - Guest

A NetBIOS share has been found which allows full access to Guest users. If the Guest account is enabled, anyone can access the computer without a valid account or password. If found on a version of Windows NT 4.0 prior to Service Pack 3, an attacker can use shares to cause the machine to crash.

Risk: High

OS Vulnerable: Windows NT

Fix: Disable the guest account, correct the share permissions, or remove the share.

Disable the guest account as follows:

1. [Start the User Manager.](#)

2. Select the guest account.
3. From the **User** menu, choose **Properties**.
4. Select the **Accounts Disabled** checkbox.

-OR-

Set the permissions explicitly as follows:

1. Navigate to the share in Windows Explorer.
2. Right-click the share, select **Properties**.
3. Under the **Sharing** tab, review the permissions.
4. Allow access only to approved users.
5. Click **OK**.

-OR-

Open the command line, remove the share as follows:

1. From the **Start** menu, select **Run**.
2. Type **cmd**, then click **OK**. This opens the command line.
3. Type **net share sharename /delete**, where sharename is the name of the share.
4. Type **exit** to return to the Windows NT desktop.

All Access NetBIOS Share Found

A NetBIOS share was found which has no password required for full access. In some cases, an attacker can use these shares to gain access to the entire hard drive. NOTE: In some cases, machines running Samba will show false positives.

Risk: High

OS Vulnerable: Windows NT

Fix: Remove the share.

Remove the share as follows:

1. From the **Start** menu, select **Run**.
2. Type **cmd**, then click **OK**. This opens the command line.
3. Type **net share sharename /delete**, where sharename is the name of the share.
4. Type **exit** to return to the Windows NT desktop.

DNS Version Denial Of Service

This version of Windows NT DNS is vulnerable to denial of service and spoofing attacks. These attacks are known as [IP Spoofing](#) and allow an intruder to access sensitive information.

Risk: Medium

OS Vulnerable: Windows NT

Fix: [Apply the latest Windows NT 4.0 Service Pack.](#)

For more information, see Microsoft Knowledge Base article [Q142047.txt](#) and [Q162927.txt](#).

IIS ASP Dot Bug

This version of IIS (Internet Information Server) displays the source to active server pages (.asp files) if a period is appended to the URL. Scripting information, as well as other data in the file, is visible.

Risk: Medium

OS Vulnerable: Windows NT

Fix: [Apply the latest Windows NT 4.0 Service Pack.](#)

Lan Manager Security

LAN Manager-style hashes are enabled for network authentication. LM hashes are relatively easily broken through a brute force attack, and the stronger Windows NT style hashes should be used. For more information see the online help topic entitled LAN Manager Security.

Risk: Low

OS Vulnerable: Windows NT

Fix: Apply the latest Windows NT 4.0 Service Pack or Windows NT 4.0 Service Pack 3 (SP3) users must apply the Im-fix.

[Apply the latest Windows NT 4.0 Service Pack](#)

-OR-

Windows NT 4.0 Service Pack 3 (SP3) Users:

Apply the Im-fix as follows:

1. From the **Start** menu, choose **Run**.
2. Type <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/lm-fix/> and press ENTER.
3. View the [README.TXT](#) for patch version and execution.

Outdated RPC Locator Service

An outdated RPC Locator service was discovered. Prior to installation of Service Pack 3, an intruder can telnet to port 135 and cause the RPCSS process to consume all available CPU.

Risk: Medium

OS Vulnerable: Windows NT

Fix: [Apply the latest Windows NT 4.0 Service Pack](#) .

Writeable NetBIOS Share - Everyone

A NetBIOS share was discovered which allows anyone with permission to access the computer to write to the share.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Set the permissions to deny write access or remove the share.

Set the permissions explicitly as follows:

1. Navigate to the share in Windows Explorer.
2. Right-click the share, select **Properties**.
3. Under the **Sharing** tab, review the permissions.
4. Allow access only to approved users.
5. Click **OK**.

-OR-

Remove the share as follows:

1. From the **Start** menu, select **Run**.
2. Type **cmd**, then click **OK**. This opens the command line.
3. Type **net share sharename /delete**, where sharename is the name of the share.
4. Type **exit** to return to the Windows NT desktop.

Writable NetBIOS Share - Guest

A NetBIOS share was discovered which allows anyone with Guest access to the computer to write to the NetBIOS share.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Set the permissions to deny write access or remove the share.

Set the permissions explicitly as follows:

1. Navigate to the share in Windows Explorer.
2. Right-click the share, select **Properties**.
3. Under the **Sharing** tab, review the permissions.
4. Allow access only to approved users.
5. Click **OK**.

-OR-

Remove the share as follows:

1. From the **Start** menu, select **Run**.
2. Type **cmd**, then click **OK**. This opens the command line.
3. Type **net share sharename /delete**, where sharename is the name of the share.
4. Type **exit** to return to the Windows NT desktop.

Writeable NetBIOS Share Found

A NetBIOS share has been found which has no password required for write access. In some cases, an attacker can use these shares to gain access to the entire hard disk. Due to the fact that anyone is allowed write access with no verification of user or password, this is considered a high risk vulnerability.

Risk: High

OS Vulnerable: OS/2, Unix samba, Windows 95, Windows for Workgroups

Fix: Remove the share.

Remove the share as follows:

1. From the **Start** menu, select **Run**.
2. Type **cmd**, then click **OK**. This opens the command line.
3. Type **net share sharename /delete**, where sharename is the name of the share.
4. Type **exit** to return to the Windows NT desktop.

Default NT Administrator UserID Exists

An account named Administrator was found. This default account cannot be locked out by too many incorrect login attempts, and can be vulnerable to a [brute force](#) attack if a poor password is chosen.

Risk: Low

OS Vulnerable: Windows NT

Fix: Rename the Administrator account, create a new Administrator account with only Guest access, remove network access for administrator, and monitor against logon attempts.

First:

Open the User Manager:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.

Next, Perform the following operations to correct this vulnerability:

Rename the Administrator account as follows:

1. Select the Administrator account.
2. From the **User** menu, select **Rename**.
3. Under **Change to**, type the new name of the administrator account.
4. Click **OK**.

-AND-

Create a new Administrator account as follows:

1. From the **User** menu, choose **New User**.
2. Under **Username**, enter **Administrator**.
3. Under **Password**, type a new password for the **Administrator** account.
4. Under **Confirm Password**, confirm the new password.
5. Click **Groups**.
6. Assign this account only to the guest group.
7. Click **OK**.

-AND-

Remove network access for administrator as follows:

1. Select the Guest account.
2. From the **Policies** menu, choose **User Rights**.
3. Under **Right**, choose the **Access this computer from network**.
4. Under **Grant To**, select **Administrators**.
5. Click **Remove**.

-AND-

Enable auditing for login attempts as follows:

1. From the **Policies** menu, choose **Audit**.
2. Enable **Audit These Events**.
3. Enable **Failure** for **Logon and Logoff**.
4. Click **OK**.
5. From the **Start** menu, choose **Programs, Administrative Tools (Common), Event Viewer**.
6. From the **Log** menu, choose **Security**.
7. Monitor attempts to log in as Administrator very carefully.

Readable NT Application Log

This vulnerability enables an intruder to read the Application Log on a Windows NT computer. This may indicate that the Guest account is enabled, possibly with network access rights. If the user running the scan is an authorized user, this may not indicate a vulnerability.

Risk: Low

OS Vulnerable: Windows NT

Fix: Remove network access from guests.

Remove network access for guests as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the Policies menu, choose **User Rights**.
3. Under **Right**, choose the **Access this computer from network**.
4. Under **Grant To**, select **Guests**.
5. Click **Remove**.

Open Defaults Found Through FTP

An open account was found on the system through FTP. Default accounts through FTP allow intruders easy access to remote systems.

Risk: High

OS Vulnerable: Any

Fix: Disable the open account or change the password to something difficult to guess.

Disable the open account as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the open account.
3. From the **User** menu, choose **Properties**.
4. Select the **Accounts Disabled** checkbox.

-OR-

Change the 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 **Properties**.
4. Under **Password**, change the password.
5. Under **Confirm Password**, confirm the password.
6. Click **OK**.

Files Obtained

An open account was found on the system through FTP. Default accounts through FTP allow intruders easy access to remote systems.

Risk: Medium

OS Vulnerable: Any

Fix: View the reports to correct vulnerabilities of which the following types of files were obtained:

- [ftp](#)
- [rexec](#)
- rlogin
- rsh
- telnet
- tftp
- nis

Fixing the above corrects this vulnerability.

Finger Service

The Finger service was found running. Finger gives an intruder information such as login accounts and trusted hosts.

Risk: Low

OS Vulnerable: Any

Fix: Disable the Finger service.

Disable Finger service as follows:

1. From the **Start** menu, choose **Settings, Control Panel, Services**.
2. Under **Services**, select **Finger**.
3. Click **Stop**.

Anonymous FTP Enabled

Anonymous FTP is enabled. If FTP services are present, allowing only anonymous access prevents valid user-password pairs from being passed across the network. Proper configuration of the FTP server is critical. If an anonymous login is permitted, the Scanner attempts to copy /etc/passwd. If the FTP server is properly chrooted, /etc/passwd is not available.

Risk: Low

OS Vulnerable: Any

Fix: Disable the FTP service.

Disable FTP service as follows:

1. From the **Start** menu, choose **Settings, Control Panel, Services**.
2. Under **Services**, select **FTP**.
3. Click **Stop**.

Writeable FTP directories

Writeable FTP directories were found, which can be used as drop points for illegal material. It is also possible to inflict a denial of service attack by filling up the hard disk.

Risk: Medium

OS Vulnerable: Any

Fix: Remove writable access to FTP directories or disable the FTP service.

To remove writable access to FTP directories, contact your FTP vendor for information or refer to your FTP vendor documentation.

To find your FTP vendor and version you must ftp yourself as follows:

1. From the **Start** menu, choose **Run**.
2. Type **ftp computername** where **computername** is the name of your computer.

The vendor and version banner is then displayed.

-OR-

Disable FTP service as follows:

1. From the **Start** menu, choose **Settings, Control Panel, Services**.
2. Under **Services**, select **FTP**.
3. Click **Stop**.

Advisories: CIAC: [Wide-spread Attacks on Anonymous FTP Servers](#)

FTP Site Exec Vulnerable

A vulnerable version of Wu-FTP daemon was found. Site Exec in older versions of Wu-FTP daemon allowed root access remotely, without anonymous FTP or a regular account to exploit.

Risk: High

OS Vulnerable: Wu-FTP 2.4.1 and earlier

Fix: Upgrade your FTP server.

Upgrade to the latest version of Wu-FTP as follows:

1. Open your browser.
2. Enter this URL: <http://ftp.academ.com/academ/wu-ftpd/release.html>
3. Download the **Wu-FTP** patch

Windows NT Guest Account Enabled

The Guest account is enabled on the scanned host. A Guest account typically has too much access to the computer, since Guest is a member of the Everyone group.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Disable the guest account.

Disable the guest account as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the guest account.
3. From the **User** menu, choose **Properties**.
4. Select the **Accounts Disabled** checkbox.

Windows NT Kernel Outdated

This system was found to have an outdated Windows NT kernel version. Windows NT can allow a user to start a high priority process which cannot be killed from the Task Manager. It is extremely difficult to cause this to occur remotely.

Risk: Low

OS Vulnerable: Windows NT

Fix: Apply the latest Windows NT 4.0 Service Pack or Windows NT 4.0 Service Pack 3 (SP3) users must apply the getadmin hot-fix.

[Apply the latest Windows NT 4.0 Service Pack](#)

-OR-

Apply getadmin fix as follows:

1. From the **Start** menu, choose **Run**.
2. Type <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/getadmin-fix> and press **ENTER**.
3. View the README.TXT for patch version and execution.

Lockout Threshold Incorrect

The lockout threshold is greater than the security policy requires. This allows an intruder to attempt a Brute Force attack on any account. If the lockout period is too long, an intruder can use this as a denial of service attack.

Risk: Low

OS Vulnerable: Windows NT

Fix: Enable account lockouts after five incorrect login attempts.

Enable account lockouts as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **Account**. This opens the **Account Policy** dialog.
3. Enable **Account Lockout**.
4. Configure to lockout after 5 bad login attempts.
5. Under **Lockout Duration**, configure duration for 30 minutes.
6. Click **OK**.

Windows 95 Password Cache Files Accessible

Windows 95 caches passwords on the hard drive in files with the extension .PWL. These password cache files are weakly encrypted and easily broken, and as such should not be accessible on a shared file system.

Risk: Medium

OS Vulnerable: Windows 9x, Windows for Workgroups 3.11

Fix: Turn off file sharing on the host if it is not needed, or restrict sharing to the parts of the drive that are necessary to be shared and apply the latest Windows NT 4.0 Service Pack.

Set share permissions as follows:

1. Navigate to the share in **Windows Explorer**.
2. Right-click the share, select **Properties**.
3. Under the **Sharing** tab, review the permissions.
4. Allow write access only to approved users.
5. Click **OK**.

-AND-

[Apply the latest Windows NT 4.0 Service Pack](#)

Windows NT Minimum Password Length

The scanner has detected that the host has an allowable minimum password length that is less than the value specified on the current policy. In general, passwords shorter than 7 characters are especially susceptible to brute force attack.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Set the minimum password length to the value defined in the policy.

Set the minimum password length as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **Account**. This opens the **Account Policy** dialog.
3. Under **Minimum Password Length**, set to the value defined in the policy.
4. Click **OK**.

Repair Directory Readable

The %systemroot\repair directory is by default readable by everyone. It is possible to extract usernames and potentially the hashes of the passwords from the .sam file. Set the permissions on this directory to full control for administrators and system and remove permissions for everyone.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Restrict access to the %systemroot\repair directory to administrators only.

Restrict access from the Windows NT desktop:

1. From Windows Explorer, right-click the selected directory and select **Properties**.
2. Under the **Security** tab, click **Permissions**.
3. Configure **Administrators** with **Full Control** and every one else with **No Access**.

-OR-

Open the command line and restrict access:

1. From the **Start** menu, select **Run**.
2. Type **cmd**, then click **OK**. This opens the command line.
3. Type **cacls c:\winnt\repair /g administrators:F**.
4. Type **exit** to return to the Windows NT desktop.

Windows NT Security Log Accessible

This vulnerability enables an intruder to read the Security Log on a Windows NT computer. This indicates that the user has administrative access, and that possibly the Guest account is enabled with network access. If the user running the scanner legitimately has administrative access to the host, this is not a vulnerability.

Risk: High

OS Vulnerable: Windows NT

Fix: Rename the Administrator account, create a new Administrator account with only Guest access, remove network access for administrator, and monitor against logon attempts.

First open the User Manager:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.

Within User Manager, the following options can be used to correct this vulnerability:

Rename the Administrator account as follows:

1. Select the Administrator account.
2. From the **User** menu, select **Rename**.
3. Under **Change to**, type the new name of the administrator account.
4. Click **OK**.

-AND-

Create a new Administrator account as follows:

1. From the **User** menu, choose **New User**.
2. Under **Username**, enter **Administrator**.
3. Under **Password**, type a new password for the Administrator account.
4. Under **Confirm Password**, confirm the new password.
5. Click **Groups**.
6. Assign this account only to the guest group.
7. Click **OK**.

-AND-

Remove network access for administrator as follows:

1. Select the guest account.
2. From the **Policies** menu, choose **User Rights**.
3. Under **Right**, choose the **Access this computer from network**.
4. Under **Grant To**, select **Administrators**.
5. Click **Remove**.

-AND-

Enable auditing for login attempts as follows:

1. From the **Policies** menu, choose **Audit**.
2. Enable **Audit These Events**.
3. Enable **Failure** for **Logon and Logoff**.
4. Click **OK**.
5. From the **Start** menu, choose **Programs, Administrative Tools (Common), Event Viewer**.
6. From the Log menu, choose **Security**.
7. Monitor attempts to log in as Administrator very carefully.

Windows NT System Log Accessible

Windows NT System Log was found to be accessible. This vulnerability enables an intruder to read the System Log on a Windows NT computer. This may indicate that the guest account is enabled, possibly with network access rights. If the user running the scan is an authorized user, this may not indicate a vulnerability.

Risk: Low

OS Vulnerable: Windows NT

Fix: Remove network access for administrator.

Remove network access for administrator as follows:

1. Select the guest account.
2. From the **Policies** menu, choose **User Rights**.
3. Under **Right**, choose the **Access this computer from network**.
4. Under **Grant To**, select **Administrators**.
5. Click **Remove**.

Windows NT Guest User Has Blank Password

The Guest account is enabled and has no password. This allows someone to log in to the host with any user name and any password.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Set the Guest password to a minimum length of seven characters

Set the minimum password length as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select Guest.
3. From the Policies menu, choose **Account**. This opens the **Account Policy** dialog.
4. Under **Minimum Password Length**, configure at least 7 characters.
5. Click **OK**.

Windows NT Administrator Has Blank Password

The scanner detected an Administrator account with no password. Some vendors have recently begun shipping Windows NT pre-installed with no password on the Administrator account.

Risk: High

OS Vulnerable: Windows NT

Fix: Set the Administrator password to a minimum length of seven characters and change the password.

Set the minimum password length as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select administrator.
3. From the **Policies** menu, choose **Account**.
4. Under **Minimum Password Length**, configure at least 7 characters.
5. Click **OK**.

-AND-

Change the password as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select administrator.
3. From the **User** menu, choose **Properties**.
4. Under **Password**, change the password.
5. Under **Confirm Password**, confirm the password.
6. Click **OK**.

Windows NT Administrator Has No Password

The scanner detected an Administrator account with no password. Some vendors have recently begun shipping Windows NT pre-installed with no password on the Administrator account.

Risk: High

OS Vulnerable: Windows NT

Fix: Set the Administrator password to a minimum length of seven characters and change the password.

Set the minimum password length as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select administrator.
3. From the **Policies** menu, choose **Account**.
4. Under **Minimum Password Length**, configure at least 7 characters.
5. Click **OK**.

-AND-

Change the password as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select administrator.
3. From the **User** menu, choose **Properties**.
4. Under **Password**, change the password.
5. Under **Confirm Password**, confirm the password.
6. Click **OK**.

Windows NT User Has No Password

The scanner detected a User account with no password. An attacker could use this account to gain access to sensitive information.

Risk: High

OS Vulnerable: Windows NT

Fix: Set the User password to a minimum length of seven characters and change the password.

Set the minimum password length as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select user.
3. From the **Policies** menu, choose **Account**.
4. Under **Minimum Password Length**, configure at least 7 characters.
5. Click **OK**.

-AND-

Change the password as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select user.
3. From the **User** menu, choose **Properties**.
4. Under **Password**, change the password.
5. Under **Confirm Password**, confirm the password.
6. Click **OK**.

Windows NT Guest Has No Password

The scanner detected a Guest account with no password. An attacker could use this account to gain access to sensitive information.

Risk: High

OS Vulnerable: Windows NT

Fix: Set the guest password to a minimum length of seven characters and change the password.

Set the minimum password length as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select guest.
3. From the **Policies** menu, choose **Account**.
4. Under **Minimum Password Length**, configure at least 7 characters.
5. Click **OK**.

-AND-

Change the password as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select guest.
3. From the **User** menu, choose **Properties**.
4. Under **Password**, change the password.
5. Under **Confirm Password**, confirm the password.
6. Click **OK**.

User Account Has Blank Password

The scanner detected a User account with no password. An attacker could use this account to gain access to sensitive information.

Risk: High

OS Vulnerable: Windows NT

Fix: Set the User password to a minimum length of seven characters and change the password.

Set the minimum password length as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select user.
3. From the **Policies** menu, choose **Account**.
4. Under **Minimum Password Length**, configure at least 7 characters.
5. Click **OK**.

-AND-

Change the password as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select user.
3. From the **User** menu, choose **Properties**.
4. Under **Password**, change the password.
5. Under **Confirm Password**, confirm the password.
6. Click **OK**.

Administrator Account Has Password The Same As The Account Name

The scanner detected an Administrator account with the password set to the account name. An attacker could use this account to gain access to sensitive information.

Risk: High

OS Vulnerable: Windows NT

Fix: Set the administrator password to a minimum length of seven characters and change the password.

Set the minimum password length as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select administrator.
3. From the **Policies** menu, choose **Account**.
4. Under **Minimum Password Length**, configure at least 7 characters.
5. Click **OK**.

-AND-

Change the password as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select administrator.
3. From the **User** menu, choose **Properties**.
4. Under **Password**, change the password.
5. Under **Confirm Password**, confirm the password.
6. Click **OK**.

Guest Account Has A Password The Same As The Account Name

The scanner detected a Guest account with the password set to the account name. An attacker could use this account to gain access to sensitive information.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Set the guest password to a minimum length of seven characters and change the password.

Set the minimum password length as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select guest.
3. From the **Policies** menu, choose **Account**.
4. Under **Minimum Password Length**, configure at least 7 characters.
5. Click **OK**.

-AND-

Change the password as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select guest.
3. From the **User** menu, choose **Properties**.
4. Under **Password**, change the password.
5. Under **Confirm Password**, confirm the password.
6. Click **OK**.

User Account Has a Password the Same as the Account Name

The scanner detected a User account with the password set to the account name. An attacker could use this account to gain access to sensitive information.

Risk: High

OS Vulnerable: Windows NT

Fix: Set the user password to a minimum length of seven characters and change the password.

Set the minimum password length as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select user.
3. From the **Policies** menu, choose **Account**.
4. Under **Minimum Password Length**, configure at least 7 characters.
5. Click **OK**.

-AND-

Change the password as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select user.
3. From the **User** menu, choose **Properties**.
4. Under **Password**, change the password.
5. Under **Confirm Password**, confirm the password.
6. Click **OK**.

Shares Enumerated Through A Null Session

Users or shares were detected on this host using a null session. A null session is a NetBIOS connection established with a zero length string as user, password, and domain name, which is designed to enable enumeration of shares and users. This capability has always been present in Windows NT, but was recently discovered to allow access to the registry with the same level of permissions as the Everyone group. It is a low risk vulnerability (similar to finger) that allows users and shares to be enumerated.

Risk: Medium

OS Vulnerable: Windows 9x, Windows NT

Fix: To remove the vulnerability, Windows NT users must restrict anonymous connections. Windows NT users should remove all unnecessary shares and apply the sec-fix patch described later in this section. Windows 95 users must remove all shares to avoid flagging this vulnerability. If shares are needed and must be secure, consider upgrading to Windows NT running NTFS.

Windows 9x:

Remove all shares or upgrade to Windows NT. Windows 9x provides no way to resolve this vulnerability, and the vulnerability will be flagged if any shares are detected, even if they are not accessible.

Windows 9x and Windows NT:

To remove a share from the command line:

1. From the Start menu, type cmd.
2. Click OK.
3. Type: net share sharename /delete.
4. Press Enter.

Windows NT 4.0 with Service Pack 2 (SP2):

Apply sec-fix as follows:

1. From the **Start** menu, choose **Run**.
2. Type <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP2/sec-fix/> and click **OK**.

View README.TXT for version and execution.

-OR-

[Apply the latest Windows NT 4.0 Service Pack](#)

-AND-

Regulate access to the NT registry as follows:

WARNING: Incorrectly using Registry Editor may cause severe and irreparable damage and may require you to reinstall your operating system. Internet Security Systems cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA**.
4. On the **Edit** menu, click **Add Value** and use the following entries:
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Value: 1.
5. Reboot the system to apply the changes.

WARNING: The winreg key will not be present if Service Pack 3 is not installed. Resetting the Registry entries

is only effective after the patch or Service Pack 3 have been applied. For more information see Microsoft Knowledge Base article Q155363.

Users Enumerated through a Null Session

Users were enumerated through a null session. Account names may be acquired, providing the foundation for a Brute Force attack.

Risk: Medium

OS Vulnerable: Any

Fix: Apply the latest Windows NT 4.0 Service Pack and regulate access to the NT registry , or Windows NT 4.0 Service Pack 2 (SP2) user must apply the sec-fix patch, and regulate access to the NT registry.

[Apply the latest Windows NT 4.0 Service Pack](#)

-OR-

Apply sec-fix as follows:

1. From the **Start** menu, choose **Run**.
2. Type <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP2/sec-fix/> and click **OK**.
3. View README.TXT for version and execution.

-AND-

Regulate access to the NT registry as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA**.
4. On the **Edit** menu, click **Add Value** and use the following entries:

Value Name: RestrictAnonymous

Data Type: REG_DWORD

Value: 1.

5. Reboot the system to apply the changes.

WARNING: The winreg key will not be present if Service Pack 3 is not installed. Resetting the Registry entries is only effective after the patch and Service Pack 3 have been applied. For more information see Microsoft Knowledge Base article Q155363.

Missing Post-SP2 Security Patches

This check detects the application of post-Service Pack 2 security patches, which fix a number of network vulnerabilities. Service Pack 3 contains this patch. **WARNING:** Service Pack 2 must be applied before applying this patch. Do not apply this patch directly over Service Pack 1, or you will cause the machine to crash. Service Pack 3 may be applied over any configuration. These patches are documented in the following Microsoft Knowledge Base articles Q143474, Q143475, and Q161372, at <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP2/sec-fix/>.

Risk: Medium

OS Vulnerable: Windows NT

Fix: [Apply the latest Windows NT 4.0 Service Pack](#)

Out of Band DoS

This system was found to be vulnerable to the OOB denial-of-service attack on port 139. As documented in Microsoft Knowledge Base article [Q143478](#), sending out of band data to port 139 will cause Windows NT to crash and Windows 9x to lose networking and possibly crash.

Risk: Medium.

OS Vulnerable: Windows NT, Windows 9x

Fix: Apply the latest Windows NT 4.0 Service Pack or Windows NT 4.0 Service Pack 3 (SP3) users must apply the teardrop2 patch.

[Apply the latest Windows NT 4.0 Service Pack](#)

-OR-

Windows NT 4.0 Service Pack 3 (SP3) Users:

Apply teardrop2 as follows:

1. From the **Start** menu, choose **Run**.
2. Type '<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/>' and press **ENTER**.
3. View the README.TXT for patch version and execution.

For more information about teardrop2, see Microsoft Knowledge Base article Q179129 at <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/Q179129.txt>

Missing Syncstorm patch

The scanner achieves a temporary denial of service attack by spoofing a large number of TCP connections to the target. Syn attacks can target an entire machine, or a specific TCP service. This system was found to be vulnerable to Syn Storm. Sending a Sync to a host indicates that the source wishes to start a connection with the destination. Each Sync that is received by the kernel requires an allocation of buffer space to manage the connection establishment. By sending a number of Syncs without actually establishing a connection, these buffers can be very quickly filled, leaving no space for real connections to be established until the fake Syncs time out.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Apply the latest Windows NT 4.0 Service Pack or Windows NT 4.0 Service Pack 3(SP3) users must apply the teardrop2 patch.

[Apply the latest Windows NT 4.0 Service Pack](#)

-OR-

Windows NT 4.0 Service Pack 3 (SP3) Users:

Apply teardrop2 as follows:

1. From the **Start** menu, choose **Run**.
2. Type '<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/>' and press **ENTER**.
3. View the README.TXT for patch version and execution.

For more information about teardrop2, see Microsoft Knowledge Base article Q179129 at <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/Q179129.txt>

Advisories: [CERT Advisory CA-96.21](#)

Missing PowerPoint Security Patch

This check detected the absence of the PowerPoint security patch. If missing, Internet Explorer will execute an application from within PowerPoint without warning the user.

Risk: Low

OS Vulnerable: Windows NT

Fix: Apply the PowerPoint (PP) security patch.

Apply the PP patch as follows:

1. Open your browser.
2. Enter this URL: <http://www.microsoft.com/msdownload/iesecurity/iepptsecurity.htm>.
3. Download the **PPTWarn.exe** patch.

Vulnerable to NetBIOS Dictionary Attack

This check performed a dictionary attack upon resources accessible through NetBIOS.

Risk: High

OS Vulnerable: Windows for Workgroups 3.11 and Windows 9x

Fix: Change your passwords so they are difficult to guess and are not a part of a password dictionary.

Change your password as follows:

1. Open the **Passwords** icon in the **Control Panel**.
2. From the **Passwords** tab, click **Change Windows Password...**
3. Under **New Password**, enter the new password.
4. Under **Confirm Password**, confirm the password.
5. Click **OK**.

Vulnerable to NetBIOS Permutations Attack

A NetBIOS share was found with a password which was guessed by iterating through all combinations of 4-letter passwords.

Risk: High

OS Vulnerable: Windows for Workgroups 3.11 and Windows 9x

Fix: Set the password to a minimum length of seven characters and change the password.

Set the minimum password length as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, choose **Account**.
4. Under **Minimum Password Length**, configure at least 7 characters.
5. Click **OK**.

-AND-

Change the 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 **Properties**.
4. Under **Password**, change the password.
5. Under **Confirm Password**, confirm the password.
6. Click **OK**.

Insecure File System

A NetBIOS share has been found where the underlying file system does not support security. The only security which can be applied to this share are share-level permissions.

Risk: Low

OS Vulnerable: OS/2, Windows NT, Windows 9x, and Windows for Workgroups 3.11

Fix: If the host is running Windows NT, convert the file system to NTFS using the 'convert' command.

Convert to NTFS as follows:

1. From the **Start** menu, choose **Run**.
2. Type **cmd** and press **ENTER**. This opens the command prompt.
3. Type **convert c: /fs:ntfs** and press **ENTER**.
4. Reboot your system.
5. Run **chkdsk** to make sure no errors are present.

If the host dual-boots into Windows 9x or an older version of Windows, you will lose the ability to boot any operating system other than Windows NT. If the host is running an operating system other than Windows NT and security is desired, upgrade to Windows NT, and convert the file system to NTFS. Consult your vendor documentation for more details.

Maximum Password Age Incorrect

The maximum password age is longer than your policy specifies. Passwords should be changed on a regular basis.

Risk: Low

OS Vulnerable: Windows NT

Fix: Configure the password age between 30 and 42 days.

Configure the password age as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, select **Account**.
4. Under **Maximum Password Age**, set the maximum password age to the value between 30 and 42 days.

Minimum Password Age Incorrect

The minimum password age is shorter than your policy specifies. Passwords should not be changed too rapidly, or some users will set a newly changed password to one they have used previously.

Risk: Low

OS Vulnerable: Windows NT

Fix: Configure the minimum password age to a value determined by your security policy. A value between 1 or 2 days is recommended.

Configure the password age as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, select **Account**.
4. Under **Minimum Password Age**, set the value determined by your security policy.

Forced Logoff Not Enabled

Forced logoffs are not enabled. If this is not enabled, users will not be forced to log out once their allowed login hours expire.

Risk: Low

OS Vulnerable: Windows NT

Fix: Enable forced logoffs.

Enable logoffs as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, choose **User Rights**.
4. Under **Right**, select **Force shutdown from a remote system**.
5. Click **Add**.

Password History Length Insufficient

The host has a password history length less than the security policy specifies. Windows NT will prevent a user from re-using the number of passwords specified by the password history length.

Risk: Low

OS Vulnerable: Windows NT

Fix: Set the password uniqueness to a value determined by your security policy.

Change the password uniqueness as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, choose **User Rights**.
4. Under **Password Uniqueness**, configure **Set Remember n Passwords** where n is a value of your security policy.

Lockout Duration Insufficient

The lockout duration is less than the value specified by the security policy. This value specifies how long an account is locked out if too many logon failures occur within the period of time specified by in the User Manager. If the duration is too short, or if account lockouts are not enabled, intruders can more easily brute force your accounts.

Risk: Low

OS Vulnerable: Windows NT

Fix: Set the lockout duration to the value required by your security policy.

Set the lockout duration as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, choose **Account**.
4. Under **Lockout Duration**, set the lockout duration to the value required by your policy.
5. Click **OK**.

Lockout Window Insufficient

The lockout observation window is less than the value specified by the security policy. This value specifies what period of time that passes between incorrect logins. If the duration is too short, or if account lockouts are not enabled, intruders can more easily brute force your accounts.

Risk: Low

OS Vulnerable: Windows NT

Fix: Set the lockout window duration to the value required by your security policy.

Set the lockout window duration as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, choose **Account**.
4. Under **Account Lockout**, configure the **reset count after n minutes**.
5. Click **OK**.

DNS Predictable Query

An unpatched version of Windows NT DNS has been found. If the DNS query numbers are predictable, it is possible for an attacker to spoof replies to DNS queries, which could potentially redirect traffic to hostile sites. See Microsoft Knowledge base article Q167629 for details.

Risk: Medium

OS Vulnerable: Windows NT

Fix: [Apply the latest Windows NT 4.0 Service Pack.](#)

IIS CGI Overflow

An unpatched version of Windows NT Internet Information Server has been found. It is possible for an attacker to cause the server to fail by sending it an overly large CGI request. See Microsoft Knowledge base article Q143484 for details.

Risk: Medium

OS Vulnerable: Windows NT

Fix: [Apply the latest Windows NT 4.0 Service Pack.](#)

Getadmin Patch Not Applied

An unpatched version of Windows NT has been found. It is possible for a local user to obtain administrator privileges by running getadmin. See Microsoft Knowledge base article Q146965 for details.

Risk: High

OS Vulnerable: Windows NT

Fix: Apply the latest Windows NT 4.0 Service Pack or Windows NT 4.0 Service Pack 3 (SP3) users must apply the getadmin hot-fix.

[Apply the latest Windows NT 4.0 Service Pack](#)

-OR-

Windows NT 4.0 Service Pack 2 (SP2) Users:

Apply getadmin fix as follows:

1. From the **Start** menu, choose **Run**.
2. Type <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/getadmin-fix> and press **ENTER**.
3. View the README.TXT for patch version and execution.

Ssping Patch Not Applied

An unpatched version of Windows NT has been found. It is possible for an attacker to cause the host to crash by sending improperly formed ICMP packets. See Microsoft Knowledge base article Q154174 for details.

Risk: Medium.

OS Vulnerable: Windows NT

Fix: Apply the teardrop2 patch.

Apply teardrop2 as follows:

1. From the **Start** menu, choose **Run**.
2. Type '<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/>' and press **ENTER**.
3. View the README.TXT for patch version and execution.

For more information about teardrop2, see Microsoft Knowledge Base article Q179129 at <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/Q179129.txt>

Chargen Patch Not Applied

An unpatched version of Windows NT Simple TCP/IP services has been found. It is possible for an attacker to cause a network denial of service by sending broadcast UDP packets to the Windows NT chargen service. See Microsoft Knowledge base article Q154460 for details.

Risk: Medium

OS Vulnerable: Windows NT

Fix: [Apply the latest Windows NT 4.0 Service Pack.](#)

WINS Patch Not Applied

An unpatched version of Windows NT WINS has been found. It is possible for an attacker to cause WINS to fail by sending invalid UDP packets. See Microsoft Knowledge base article Q155701 for details.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Apply the post-SP3 wins-udp patch, or SP4 when available.

Apply the post-sp3 wins-udp patch as follows:

1. From the **Start** menu, choose **Run**.
2. Type <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/winsupd-fix/> and click **OK**.
3. View the README.TXT for patch version and execution.

Refer to article Q155701 located in the same directory for more information.

Guessed Windows NT Administrator Password

The password on the Administrator Account for this host has been guessed. An intruder can gain access to sensitive system files. This is considered a high risk vulnerability.

Risk: High

OS Vulnerable: Windows NT

Fix: Set the administrator password to a minimum length of seven characters and change the password.

Set the minimum password length as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select administrator.
3. From the **Policies** menu, choose **Account**.
4. Under **Minimum Password Length**, configure at least 7 characters.
5. Click **OK**.

-AND-

Change the password as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select administrator.
3. From the **User** menu, choose **Properties**.
4. Under **Password**, change the password.
5. Under **Confirm Password**, confirm the password.
6. Click **OK**.

Guessed Windows NT Account Password

The password on a User Account for this host has been guessed. An intruder can gain access to sensitive system files. This is considered a high risk vulnerability.

Risk: High

OS Vulnerable: Windows NT

Fix: Set the User password to a minimum length of seven characters and change the password.

Set the minimum password length as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select user.
3. From the **Policies** menu, choose **Account**.
4. Under **Minimum Password Length**, configure at least 7 characters.
5. Click **OK**.

-AND-

Change the password as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select user.
3. From the **User** menu, choose **Properties**.
4. Under **Password**, change the password.
5. Under **Confirm Password**, confirm the password.
6. Click **OK**.

Guessed Windows NT Guest Password

The password on the Guest Account for this host has been guessed. An intruder can gain access to sensitive system files.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Set the Guest password to a minimum length of seven characters and change the password.

Set the minimum password length as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select guest.
3. From the **Policies** menu, choose **Account**.
4. Under **Minimum Password Length**, configure at least 7 characters.
5. Click **OK**.

-AND-

Change the password as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select guest.
3. From the **User** menu, choose **Properties**.
4. Under **Password**, change the password.
5. Under **Confirm Password**, confirm the password.
6. Click **OK**.

Permanent Account Lockout

Permanent lockouts have been enabled on this host, and the user list was obtained via a null session. An intruder could engage in password guessing attacks and lock out all users in that domain or host.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Enable Restrict Anonymous in the registry and/or set the account lockout duration to some fixed value.

Enable Restrict Anonymous as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the registry editor.
3. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA**.
4. From the **Edit** menu, choose **Add Value**.
5. Add the following entry:
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Value: 1'

-AND/OR-

Set the lockout duration as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, choose **Account**.
4. Under **Lockout Duration**, set the lockout duration to the value required by your policy.
5. Click **OK**.

Land Denial of Service Attack

The scanner discovered an outdated version of tcpip.sys. This vulnerability allows an attacker to cause a high CPU load by sending a spoofed packet to a port which claims to have originated from that port. Variations on this attack can cause Windows NT machines to lock up. For more information see Microsoft Knowledge Base article Q165005.

Risk: Low

OS Vulnerable: Any

Fix: Apply the teardrop2 patch.

Apply teardrop2 as follows:

1. From the **Start** menu, choose **Run**.
2. Type '<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/>' and press **ENTER**.
3. View the README.TXT for patch version and execution.

Note: Applying router of firewall rules which deny all incoming packets which claim to originate from the internal network is good practice, and will stop this attack.

For more information about teardrop2, see Microsoft Knowledge Base article **Q179129** at <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/Q179129.txt>.

URL Security Zone Signed Active X Download

Allows signed ActiveX controls to be downloaded directly from the URL security zone of the HTML page that contains the control. Potentially malicious ActiveX controls may be automatically downloaded.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT

Fix: Disable 'Download signed Active X controls' on IE 4.x.

Disable 'Download signed Active X controls' as follows:

1. Open Internet Explorer 4.x.
2. From the **View** menu, choose **Internet Options**.
3. Click the **Security** tab.
4. Under **Internet Zone**, click **Custom (for expert users)**.
5. Click **Settings**.
6. Under **ActiveX Controls and plugins**, navigate to **Download signed ActiveX controls**.
7. Click **Disable**.
8. Click **OK**.

URL Security Zone Unsigned Active X Download.

Allows unsigned ActiveX controls to be downloaded directly from the URL security zone of the HTML page that contains the control. Potentially malicious ActiveX controls may be automatically downloaded.

Risk: Medium

OS Vulnerable: Windows 9x, Windows NT 4.0 with Internet Explorer 4.x installed.

Fix: Disable 'Download unsigned Active X controls' on IE 4.x.

Disable 'Download unsigned Active X controls' as follows:

1. Open Internet Explorer 4.x.
2. From the **View** menu, choose **Internet Options**.
3. Click the **Security** tab.
4. Under **Internet Zone**, click **Custom (for expert users)**.
5. Click **Settings**.
6. Under **ActiveX Controls and plugins**, navigate to **Download unsigned ActiveX controls**.
7. Click **Disable**.
8. Click **OK**.

URL Security Zone scripting safe Active X controls.

Allows ActiveX controls marked as safe to be scripted from the URL security zone of the HTML page that contains the script. Potentially malicious scripts containing ActiveX controls may be automatically executed by the browser.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT

Fix: Disable 'Download unsigned Active X controls' on IE 4.x.

Disable 'Script Active X controls marked safe for scripting' as follows:

1. Open Internet Explorer 4.x.
2. From the **View** menu, choose **Internet Options**.
3. Click the **Security** tab.
4. Under **Internet Zone**, click **Custom (for expert users)**.
5. Click **Settings**.
6. Under **ActiveX Controls and plugins**, navigate to **Script Active X controls marked safe for scripting**.
7. Click **Disable**.
8. Click **OK**.

URL Security Zone scripting of unsafe Active X controls.

Allows ActiveX controls not marked as safe to be automatically initialized and executed from the URL security zone of the HTML page that contains the script. Potentially malicious scripts containing ActiveX controls may be automatically executed by the browser.

Risk: Medium

OS Vulnerable: Windows 9x, Windows NT

Fix: Disable 'Initialize and script Active X controls not marked as safe' on IE 4.x.

Disable "Initialize and script Active X controls not marked as safe" as follows:

1. Open Internet Explorer 4.x.
2. From the **View** menu, choose **Internet Options**.
3. Click the **Security** tab.
4. Under **Internet Zone**, click **Custom (for expert users)**.
5. Click **Settings**.
6. Under **ActiveX Controls and plugins**, navigate **Initialize and script Active X controls not marked as safe**.
7. Click **Disable**.
8. Click **OK**.

URL Security Zone Active X Execution

Allows ActiveX controls and plug-ins to be launched from the URL security zone of the HTML page that contains the control.

Risk: Medium

OS Vulnerable: Windows 9x, Windows NT

Fix: Disable 'Run Active X controls and Plug-ins' on IE 4.x.

Disable 'Run Active X controls and Plug-ins' as follows:

1. Open Internet Explorer 4.x.
2. From the **View** menu, choose **Internet Options**.
3. Click the **Security** tab.
4. Under **Internet Zone**, click **Custom (for expert users)**.
5. Click **Settings**.
6. Under **ActiveX Controls and plugins**, navigate to **Run Active X controls and Plug-ins**.
7. Click **Disable**.
8. Click **OK**.

URL Security Zone Auto user authentication

Allows the browser to automatically transmit the user's credentials when requested from an HTML page in the selected URL security zone. A potentially malicious web site may automatically obtain the user's credentials without the user's knowledge.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT 4.0

Fix: Disable 'Automatic logon with current username and password' on IE 4.x.

Disable 'Automatic logon with current username and password' as follows:

1. Open Internet Explorer 4.x.
2. From the **View** menu, choose **Internet Options**.
3. Click the **Security** tab.
4. Under **Internet Zone**, click **Custom (for expert users)**.
5. Click **Settings**.
6. Under **User Authentication**, navigate to **Automatic logon with current username and password**.
7. Click **Disable**.
8. Click **OK**.

URL Security Zone file download

Allows files to be downloaded directly from the URL security zone of the HTML page containing the download link. A potentially malicious or virus-infected program may be received without the user's knowledge.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT

Fix: Disable 'File download' on IE 4.x.

Disable 'File download' as follows:

1. Open Internet Explorer 4.x.
2. From the **View** menu, choose **Internet Options**.
3. Click the **Security** tab.
4. Under **Internet Zone**, click **Custom (for expert users)**.
5. Click **Settings**.
6. Under Downloads, navigate to **File Download**.
7. Click **Disable**.
8. Click **OK**.

URL Security Zone low java permissions

Allows Java applets to operate out of the Java sandbox model, so that they will be allowed to perform high-capability operations, such as file I/O operations. A potentially malicious Java applet may perform unauthorized modifications to the machine.

Risk: Medium

OS Vulnerable: Windows 9x, Windows NT 4.0

Fix: Set Java Permissions to 'High safety' in IE 4.x.

Set Java Permissions as follows:

1. Open Internet Explorer 4.x.
2. From the **View** menu, choose **Internet Options**.
3. Click the **Security** tab.
4. Under **Internet Zone**, click **Custom (for expert users)**.
5. Click **Settings**.
6. Under **Java**, navigate to **Java Permissions**.
7. Click **High Safety**.
8. Click **OK**.

URL Security Zone low channel permissions

Allows the browser to automatically install software updates from the URL security zone that contains the channel content. Potentially malicious channel content may automatically download and install without the user's knowledge.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT

Fix: Set Software Channel Permissions to 'High safety' in IE 4.x.

Set Software Channel Permissions as follows

1. Open Internet Explorer 4.x.
2. From the **View** menu, choose **Internet Options**.
3. Click the **Security** tab.
4. Under **Internet Zone**, click **Custom (for expert users)**.
5. Click **Settings**.
6. Under **Miscellaneous**, navigate to **Software Channel Permissions**.
7. Click **High Safety**.
8. Click **OK**.

URL Security Zone file launch

Allows files or applications to be launched directly from the URL security zone of the HTML page that contains the file or application. Potentially malicious files or applications may automatically execute on the browser computer.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT 4.0

Fix: Disable 'Launching applications and files in an IFRAME' in IE 4.x.

Disable 'Launching applications and files in an IFRAME' as follows:

1. Open Internet Explorer 4.x.
2. From the **View** menu, choose **Internet Options**.
3. Click the **Security** tab.
4. Under **Internet Zone**, click **Custom (for expert users)**.
5. Click **Settings**.
6. Under **Miscellaneous**, navigate to **Launching applications and files in an IFRAME**.
7. Click **Disable**.
8. Click **OK**.

URL Security Zone desktop install

Allows desktop content to be downloaded and installed directly from the URL security zone of the HTML page that contains the desktop content. Potentially malicious desktop content may automatically download and install on the machine.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT

Fix: Disable 'Installation of desktop items' in IE 4.x.

Disable 'Installation of desktop items' as follows:

1. Open Internet Explorer 4.x.
2. From the **View** menu, choose **Internet Options**.
3. Click the **Security** tab.
4. Under **Internet Zone**, click **Custom (for expert users)**.
5. Click **Settings**.
6. Under **Miscellaneous**, navigate to **Installation of desktop items**.
7. Click **Disable**.
8. Click **OK**.

URL Security Zone non-secure form submission

Allows a browser to submit non-encrypted form data to the URL security zone of the HTML page making the data request. Potentially sensitive data may be intercepted in transit by packet sniffing.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT 4.0

Fix: Disable 'Submit non-encrypted form data' in IE 4.x.

Disable 'Submit non-encrypted form data' as follows:

1. Open Internet Explorer 4.x.
2. From the **View** menu, choose **Internet Options**.
3. Click the **Security** tab.
4. Under **Internet Zone**, click **Custom (for expert users)**.
5. Click **Settings**.
6. Under **Miscellaneous**, navigate to **Submit non-encrypted form data**.
7. Click **Disable**.
8. Click **OK**.

URL Security Zone java scripting

Allows script code embedded in HTML pages within the URL security zone to be able to use Java applets, provided that the applets expose properties, methods, and events. The browser may automatically execute potentially malicious Java applets or scripts.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT

Fix: Disable 'Scripting of Java applets' in IE 4.x.

Disable 'Scripting of Java applets' as follows:

1. Open Internet Explorer 4.x.
2. From the **View** menu, choose **Internet Options**.
3. Click the **Security** tab.
4. Under **Internet Zone**, click **Custom (for expert users)**.
5. Click **Settings**.
6. Under **Scripting**, navigate to **Scripting of Java applets**.
7. Click **Disable**.
8. Click **OK**.

URL Security Zone active scripting

Allows script code embedded in HTML pages within the URL security zone to be able to use embedded objects (such as ActiveX or Java), provided that the applets expose properties, methods, and events. The browser may automatically execute potentially malicious scripts.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT

Fix: Disable 'Active scripting' in IE 4.x.

Disable 'Active scripting' as follows:

1. Open Internet Explorer 4.x.
2. From the **View** menu, choose **Internet Options**.
3. Click the **Security** tab.
4. Under **Internet Zone**, click **Custom (for expert users)**.
5. Click **Settings**.
6. Under **Scripting**, navigate to **Active scripting**.
7. Click **Disable**.
8. Click **OK**.

Using Share Level Access

Windows 9x is configured for Share Level Access. This only requires a password for authentication of share users. Selecting User Level Access uses a secure server to validate users and passwords.

Risk: Low

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#)

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local Computer** icon.
4. Choose **Network, Access Control**, and enable **User-level Access Control**.
5. Under **Settings for User-level Access Control**, select the **Authentication Type**.
6. Click **OK**.

Not Using Server Validate

Windows 9x is not configured to use a secure server to validate user logons before accessing the machine.

Risk: Medium

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to require validation by network for windows access.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local Computer** icon.
4. Choose **Network, Logon**, and enable the **Require Validation by Network for Windows Access** check box.
5. Click **OK**.

Using Domain Password Caching

Windows 9x is configured to cache domain passwords.

Risk: Medium

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to disable password caching.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local Computer** icon.
4. Choose **Network, Passwords**, and enable the **Disable Password Caching** check box.
5. Click **OK**.

Share Passwords are Not Hidden

Windows 9x is not configured to hide share passwords with asterisks as they are entered.

Risk: High

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to hide shared passwords.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local Computer** icon.
4. Choose **Network, Passwords**, and enable the **Hide shared passwords with asterisks** check box.
5. Click **OK**.

Password Caching is Enabled

Windows 9x is configured to cache passwords. These passwords are stored in an easily decrypted file.

Risk: Medium

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to disable password caching.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local Computer** icon.
4. Choose **Network, Passwords**, and enable the **Disable Password Caching** check box.
5. Click **OK**.

Password Length Too Short

Windows 9x is configured to allow passwords of less than seven characters. Such passwords are easily guessed.

Risk: Medium

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to set minimum password length.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local Computer** icon.
4. Choose **Network, Passwords**, and enable the **Minimum Windows password length** check box.
5. Under **Settings for Minimum Windows password length**, set the value to 7 or greater.
6. Click **OK**.

Dialin is Enabled

Windows 9x is configured to allow users to dial in to this machine.

Risk: Low

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to disable network dial-in.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local Computer** icon.
4. Choose **Network, Dial-Up Networking**, and enable the **Disable Dial-in** check box.
5. Click **OK**.

File Sharing is Allowed

Windows 9x is configured to allow file sharing. This allows users access to the disks on the machine.

Risk: Low

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to disable file sharing.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local Computer** icon.
4. Choose **Network, Sharing**, and enable the **Disable File Sharing** check box.
5. Click **OK**.

Print Sharing is Allowed

Windows 9x is configured to allow print sharing. This allows users access to the printers the machine.

Risk: Low

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to disable print sharing.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local Computer** icon.
4. Choose **Network, Sharing**, and enable the **Disable Print Sharing** check box.
5. Click **OK**.

Password Icon in Control Panel

Windows 9x is configured to allow the current user to access the password icon in the control panel.

Risk: Low

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to remove password icon from control panel.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local Computer** icon.
4. Choose **Network, Passwords**, and enable the **Restrict Passwords Control Panel** check box.
5. Click **OK**.

Change Password Page

Windows 9x is configured to allow the current user to access the change password page in the control panel.

Risk: Low

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to disable Passwords Control Panel.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local User** icon.
4. Choose **Control Panel, Passwords**, and enable the **Restrict Passwords Control Panel** check box.
5. Under **Settings for Restrict Passwords Control Panel**, enable the **Disable Passwords Control Panel** check box.
6. Click **OK**.

Remote Admin Page

Windows 9x is configured to allow the current user to access the Remote Administration page control panel.

Risk: Low

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to hide the remote administration page

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local User** icon.
4. Choose **Control Panel, Passwords**, and enable the **Restrict Passwords Control Panel** check box.
5. Under **Settings for Restrict Passwords Control Panel**, enable the **Hide Remote Administration Page** check box.
6. Click **OK**.

Profile Page

Windows 9x is configured to allow the current user to access the Profile page control panel.

Risk: Low

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to hide the user profiles page

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local User** icon.
4. Choose **Control Panel, Passwords**, and enable the **Restrict Passwords Control Panel** check box.
5. Under **Settings for Restrict Passwords Control Panel**, enable the **Hide User Profiles Page** check box.
6. Click **OK**.

File Sharing Enabled

Windows 9x is configured allow the current user to share files. This opens the door to an intruder providing accessibility to the shared files.

Risk: Low

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to disable file sharing controls.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local User** icon.
4. Choose **Network, Sharing**, and enable the **Disable file sharing controls** check box.
5. Click **OK**.

Print Sharing Enabled

Windows 9x is configured to allow the current user to share printers.

Risk: Low

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to disable print sharing controls.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local User** icon.
4. Choose **Network, Sharing**, and enable the **Disable print sharing controls** check box.
5. Click **OK**.

Network Access Control Page

Windows 9x is configured to allow the current user to access the Access Control page in the Network icon in the control panel.

Risk: Low

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to disable network control panel.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local User** icon.
4. Choose **Control Panel, Network**, and enable the **Restrict Network Control** check box.
5. Under **Settings for Restrict Network Control Panel**, enable the **Hide Access Control Page** check box.
6. Click **OK**.

Registry Access

Windows 9x is configured to allow the current user to edit the Registry.

Risk: Medium

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to disable the network control panel.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local User** icon.
4. Choose **Control Panel, Network**, and enable the **Restrict Network Control Panel** check box.
5. Under **Settings for Restrict Network Control Panel**, enable the **Disable Network Control Panel** check box.
6. Click **OK**.

Not Using Alphanumeric Passwords

Windows 9x is not configured to use alphanumeric passwords. Such passwords are harder to guess.

Risk: Low

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to require alphanumeric passwords.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local Computer** icon.
4. Choose **Network, Passwords**, and enable the **Require alphanumeric passwords** check box.
5. Click **OK**.

DOS Enabled

Windows 9x is configured to allow the current user to run DOS applications.

Risk: Low

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to disable the MS-DOS prompt.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local User** icon.
4. Choose **System, Restrictions**, and enable the **Disable MS-DOS prompt** check box.
5. Click **OK**.

Real Mode Enabled

Windows 9x is configured to allow the current user to run real mode DOS applications.

Risk: Low

OS Vulnerable: Windows 9x

Fix: Contact your administrator or run the [Windows 9x Policy Editor](#) to disable single mode MS-DOS applications.

Modify the policy editor as follows:

1. From the **Start** menu, choose **Programs, Accessories, System Policy Editor**.
2. From the **File** menu, choose **Open Registry**.
3. Open the **Local User** icon.
4. Choose **System, Restrictions**, and enable the **Disable single mode MS-DOS applications** check box.
5. Click **OK**.

File added since baseline scan

A new file was found in the file scan, since the baseline scan was run. This new file could be a normal file, or evil and malicious.

Risk: Medium

OS Vulnerable: Windows 9x, Windows NT.

Fix: A new file was found in the file scan, after the baseline scan was run. This new file could be a normal file, or evil and malicious.

File changed since baseline scan

A new file was changed since a baseline scan was run. This could be due to a product upgrade, or hack attempt.

Risk: High

OS Vulnerable: Windows 9x, Windows NT.

Fix: Check to see when this file was changed and what software added it.

If it is confirmed as safe, re-run the baseline scan.

{button ,JI(` sysscan.HLP>Main', `Generating_Baseline_Databases')} [More on baseline database](#)

File baseline scan was reset

This is to let the operator know that they, or someone, has reset the file baseline on their machine. This is a potential vulnerability. The scanner will not detect a [trojan horse](#) if the baseline is reset after a trojan horse is installed.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT.

Fix: Verify that the reset was legitimate. This means you know who reset it or why it was reset.

Netscape Navigator Entering a Secure Site Warning is Disabled

The browser displays no warning when entering an encrypted or secure site. A user may be unable to distinguish between viewing trusted and non-trusted content. Because this option allows pages to be decrypted without intervention, it may result in secure content being cached on the local file system in a non-secure manner.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT

Fix: Change the Navigator preferences to enable the 'Entering an encrypted site' warning.

Enable the 'Entering an encrypted site' warning as follows:

1. From the **Communicator** menu (Netscape v2, v3) or the **Window** menu (Netscape v4), choose **Security Info**.
2. Under **Security Info**, click **Navigator**.
3. Under **Show a warning before:**, enable **Entering an encrypted site**.
4. Click **OK**.

Netscape Navigator Non-secure Form Submission Warning is Disabled

The browser displays no warning when submitting non-encrypted form data to the HTML page making the data request. A user may be unable to distinguish between encrypted and non-encrypted form data. Potentially sensitive data may be intercepted by packet sniffing.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT

Fix: Change the Navigator preferences to enable the 'Sending unencrypted information to a site' warning.

Enable the ' Sending unencrypted information to a site' warning as follows:

1. From the **Communicator** menu (Netscape v2, v3) or the **Window** menu (Netscape v4), choose **Security Info**.
2. Under **Security Info**, click **Navigator**.
3. Under **Show a warning before:**, enable **Sending unencrypted information to a site**.
4. Click **OK**.

Netscape Navigator Leaving a Secure Site Warning is Disabled

The browser displays no warning when leaving an encrypted or secure site. A user may be unable to distinguish between viewing trusted and non-trusted content. Because this option allows pages to be decrypted without intervention, it may result in secure content being cached on the local file system in a non-secure manner.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT

Fix: Change the Navigator preferences to enable the 'Leaving an encrypted site' warning.

Enable the 'Leaving an encrypted site' warning as follows:

1. From the **Communicator** menu (Netscape v2, v3) or the **Window** menu (Netscape v4), choose **Security Info**.
2. Under **Security Info**, click **Navigator**.
3. Under **Show a warning before:**, enable **Leaving an Encrypted Site**.
4. Click **OK**.

Netscape Navigator Mixed Document Security Warning is Disabled

The browser displays no warning when viewing a document with both secure and insecure content. A user may be unable to distinguish between secure and insecure content.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT

Fix: Change the Navigator preferences to enable the 'Viewing a page with an encrypted/unencrypted mix' warning.

Enable the 'Viewing a page with an encrypted/unencrypted mix' warning as follows:

1. From the **Communicator** menu (Netscape v2, v3) or the **Window** menu (Netscape v4), choose **Security Info**.
2. Under **Security Info**, click **Navigator**.
3. Under **Show a warning before:**, enable **Viewing a page with an encrypted/unencrypted mix**.
4. Click **OK**.

Netscape Navigator Has Java Enabled

The browser has Java enabled. This option allows script code embedded in HTML pages to use Java applets, provided that the applets expose properties, methods, and events. The browser may automatically execute potentially malicious scripts or Java applets.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT

Fix: Change the Navigator preferences to disable 'Java'.

Disable 'Java' as follows:

Netscape Navigator v2, v3:

1. From the **Communicator** menu, choose **Security Info**.
2. Under **Security Info**, click **Java/JavaScript**.
3. Select **Java**, and click **Remove**.
4. Click **OK**.

Netscape Navigator v4:

1. From the **Edit** menu, choose **Preferences**.
2. Click on the **Advanced** option.
3. Disable the **Enable Java** check-box.
4. Click **OK**.

Netscape Navigator Has JavaScript Enabled

The browser has JavaScript enabled. This option allows the browser to automatically execute JavaScript code embedded in HTML. The browser may automatically execute potentially malicious JavaScripts.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT

Fix: Change the Navigator preferences to disable 'Java Script'.

Disable 'Java Script' as follows:

Netscape Navigator v2, v3:

1. From the **Communicator** menu, choose **Security Info**.
2. Under **Security Info**, click **Java/JavaScript**.
3. Select **Java**, and click **Remove**.
4. Click **OK**.

Netscape Navigator v4:

1. From the **Edit** menu, choose **Preferences**.
2. Click on the **Advanced** option.
3. Disable the **Enable JavaScript** check-box.
4. Click **OK**.

Bad File Version Vulnerability

This vulnerability is raised when the scanner generic file version checker detects a file which is not current.

Risk: Medium

OS Vulnerable: Windows 9x, Windows NT

Fix: Check the vendor of the file or ISS for details about the indicated file.

Install patch or upgrade from vendor. There may be a workaround.

One or More Office 97 Files are Out of date

The indicated file is known to have security risks.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT

Fix: Download the most recent Office patch from <http://www.microsoft.com/office>.

Netscape Navigator is outdated

Internet Scanner has detected an outdated version of Netscape Navigator. All versions of Navigator prior to 4.04 are known to have security issues.

Risk: Low

OS Vulnerable: Windows 9x, Windows NT

Fix: Install the latest version of Navigator.

Download Netscape Navigator as follows:

1. Open your browser.
2. Enter this address: <http://home.netscape.com/download/> .
3. Download the latest navigator.

For a list of bugs, reference: <http://home.netscape.com/assist/security/index.html> and <http://home.netscape.com/assist/security/index.html>.

TCP-IP.sys Vulnerability

The version of tcpip.sys on the machine is vulnerable to the Land exploit. Search Microsoft site on Q165005 for details.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Apply the post-SP3 land-fix.

Apply the land-fix as follows:

1. From the **Start** menu, choose **Run**.
2. Type <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/archive/land-fix/> '.
3. View the readme.txt for versions and install instructions.

Refer to Microsoft's support online (<http://www.microsoft.com/support>) articles Q165005 and Q177539 for further information.

VTCP.386 is out of date.

The version of vtcp.386 is vulnerable to the Land exploit. Search Microsoft site on Q177539 for details.

Risk: Medium

OS Vulnerable: Windows 95

Fix: Apply the post-SP3 land-fix and apply the Winsock 2 update.

Apply the land-fix as follows:

1. From the **Start** menu, choose **Run**.
2. Type <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/archive/land-fix/> .
3. View the readme.txt for versions and install instructions.
Refer to articles Q165005 and Q177539 for further information.

-AND-

Apply the Winsock 2 update as follows:

1. Open your browser.
2. Enter this address: <http://www.microsoft.com/windows/downloads/contents/Updates/W95Sockets2/default.asp>
3. Download the Winsock 2 update.

Refer to article Q177539 for more Winsock 2 information.

Winsock 2 is Not Applied.

Winsock 2 is not applied to the machine. This fixes some denial of service vulnerabilities for Windows 95.

Risk: Medium

OS Vulnerable: Windows 9x

Fix: Apply the Winsock 2 update.

Apply the Winsock 2 update as follows:

1. Open your browser.
2. Enter this address <http://www.microsoft.com/windows/downloads/contents/Updates/W95Sockets2/default.asp>
3. Download the Winsock 2 update.

Refer to article Q177539 for more Winsock 2 information.

Internet Explorer Vulnerability

The installed version of Internet Explorer is vulnerable to the following exploits:

- Buffer Overrun (95 only)
- Freiburg text-viewing
- Java-script privacy issue
- DirectX file corruption security problem

Risk: Medium

OS Vulnerable: Windows NT, Windows 9x

Fix:

Windows 95: Apply the Buffer Overrun patch, apply the Bell Labs Java-Script patch, apply the Explorer 4.0 Freiburg patch, the DirectX patch. See below.

Windows NT: Apply the Explorer 4.0 Freiburg patch, apply the Bell Labs Java-Script patch, and apply the DirectX patch. See below.

Apply the Buffer Overrun patch as follows:

1. Open your browser.
2. Enter this address: <http://www.microsoft.com/windows/ie/security/>.
3. Click **Security Issues**.
4. Download the patch.

-AND/OR-

Apply the Freiburg patch as follows:

1. Open your browser.
2. Enter this address: <http://www.microsoft.com/windows/ie/security/>.
3. Click **Security Issues**.
4. Download the patch.

-AND-

Apply the Bell Labs Java-Script patch as follows:

1. Open your browser.
2. Enter this address: <http://www.microsoft.com/windows/ie/security/>.
3. Click **Security Issues**.
4. Download the patch.

-AND-

Apply the DirectX Patch as follows:

1. Open your browser.
2. Enter this address: <http://www.microsoft.com/windows/ie/security/>.
3. Click **Security Issues**.
4. Download the patch.

IE Embed Bug

The installed version of Internet Explorer is vulnerable to the Embed bug. A malicious Web page could cause Internet Explorer 4.0 to crash through an exploit with the "EMBED" tag. It's difficult, but possible, for the page to then run code in memory on that machine.

Risk: Medium

OS Vulnerable: Windows NT, Windows 9x

Fix: Apply the Embed patch.

Apply the Embed Patch as follows:

1. Open your browser.
2. Enter this address: <http://www.microsoft.com/windows/ie/security/>.
3. Click **Security Issues**.
4. Download the patch.

IE mk bug

The installed version of Internet Explorer is vulnerable to the Mk overrun bug. This issue can cause Internet Explorer 4.0 to crash when a malicious Web site contains a certain kind of URL (that begins with "mk://") with more characters than the browser supports. The extra characters could form a malicious executable that could then run on your computer.

Risk: Medium

OS Vulnerable: Windows NT, Windows 9x

Fix: Apply the MK Overrun patch.

Apply the Make Overrun patch as follows:

1. Open your browser.
2. Enter this address: <http://www.microsoft.com/windows/ie/security/>.
3. Click **Security Issues**.
4. Download the patch.

Password Fix Not Applied

The fix for better password encryption is not applied to Windows 9x

Risk: Medium

OS Vulnerable: Windows 9x

Fix: Apply the Password Security patch.

Apply the Password Security patch as follows:

1. Open your browser.
2. Enter this address: <http://support.microsoft.com/support/kb/articles/q165/4/03.asp>.
3. Download the patch.

Novell Password Fix Not Applied

The fix for better password encryption is not applied to Windows 9x

Risk: Medium

OS Vulnerable: Windows 9x

Fix: Apply the Novell Password Security patch.

Apply the Novell Password Security patch as follows:

1. Open your browser.
2. Enter this address: <http://www.microsoft.com/Windows95/Community/MktBulletin/passwordmb.asp>
3. Download the patch.

Update to OS is Available.

A service pack of newer version of the operating system is available from Microsoft.

Risk: Medium

OS Vulnerable: Windows NT, Windows 9x

Fix: Check the Microsoft Support Web site, or with your system administrator for the latest version.

Check the Microsoft Support Web Site at: <http://support.microsoft.com/support>

Power PointViewer

This version of the PowerPoint viewer poses security risks with viewing files over the Internet. A malicious PPT presentation may launch applications without warning the user.

Risk: Low

OS Vulnerable: Windows NT, Windows 9x

Fix: Apply the Office 97 Service Release 1 (SR-1) patch or apply the Power Point patch.

Apply the SR-1 as follows:

1. Open your browser.
2. Enter this address: <http://www.microsoft.com/Office/Office97/ServiceRelease/>.
3. Download SR-1.

-OR-

Apply the PowerPoint patch as follows:

1. Open your browser.
2. Enter this address: <http://officeupdate.microsoft.com/updates/updpowerpoint.htm>
3. Download the patch.

Anti-Virus Config Changed

The installed anti-virus software's startup configuration has been changed. This indicates that the some of the anti-virus's features may be defeated.

Risk: Low

OS Vulnerable: Windows NT, Windows 9x

Fix: Reset the virus program's configuration back to the installed one or rerun the baseline scan.

[More on baseline databases](#)

Password Lockout Disabled.

The password lockout feature of NT is disabled. This allows easy brute force password cracking since accounts are never locked out.

Risk: Low

OS Vulnerable: Windows NT

Fix: Enable account lockouts after five incorrect login attempts.

Enable account lockouts as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **Account**. This opens the **Account Policy** dialog.
3. Enable **Account Lockout**.
4. Configure to lockout after 5 bad login attempts.
5. Under **Lockout Duration**, configure duration for 30 minutes.
6. Click **OK**.

No Anti-virus Software Installed

The scanner did not detect the installation of popular anti-virus software. This version of Scanner detects the following A-V packages:

- Norton AntiVirus
- McAfee VirusScan
- Incoulan (9x only)
- Dr. Solomon (9x only)
- IBM AntiVirus

Risk: Low

OS Vulnerable: Windows NT, Windows 9x

Fix: Install an anti-virus or disable this check.

Registry baseline scan was reset

This is to let the operator know that they, or someone, as reset the baseline registry scan on their machine. This is a potential vulnerability since resetting the baseline after installing a [trojan horse](#) would not pick it up.

Risk: Low

OS Vulnerable: Windows NT, Windows 9x

Fix: There is no corrective action. Verify that the baseline was legitimately reset. This means that you know who reset it or why it was reset. If the baseline reset is legitimate, this is not a vulnerability.

Registry key added since baseline scan

When scanning the configured registry keys, a new key was found since the registry baseline scan was run. This could be due to normal operations, or the installation of a [trojan horse](#).

Risk: Low

OS Vulnerable: Windows NT, Windows 9x

Fix: View the report to see which key was added. Assure its validity and reset the registry baseline.

{button ,JI(` sysscan.HLP>Main', `Generating_Baseline_Databases')} [More on baseline database](#)

Registry value added since baseline scan

When scanning the configured registry keys, a new value was found since the registry baseline scan was run. This could be due to normal operations, or the installation of a trojan horse.

Risk: Low

OS Vulnerable: Windows NT, Windows 9x

Fix: View the report to see which value was added. Assure its validity and reset the registry baseline.

{button ,JI(` sysscan.HLP>Main', `Generating_Baseline_Databases')} [More on baseline database](#)

Registry key missing since baseline scan

When scanning the configured registry keys, the indicated key was not found.. This could be due to normal operations, or someone deleting registry keys.

Risk: Low

OS Vulnerable: Windows NT, Windows 9x

Fix: View the report to see which key was removed. Assure its removal was valid and reset the registry baseline.

{button ,JI(`sysscan.HLP>Main',`Generating_Baseline_Databases')}} [More on baseline database](#)

Registry value missing since baseline scan

When scanning the configured registry keys, the indicated value was not found. This could be due to normal operations, or someone deleting registry values.

Risk: Low

OS Vulnerable: Windows NT, Windows 9x

Fix: View the report to see which value was removed. Assure its removal was valid and reset the registry baseline.

{button ,JI(`sysscan.HLP>Main',`Generating_Baseline_Databases')} [More on baseline database](#)

Registry value changed since baseline scan

When scanning the configured registry keys, the indicated value was changed since the registry baseline scan was run. This could be due to normal operations, or someone maliciously changing registry values.

Risk: Low

OS Vulnerable: Windows NT, Windows 9x

Fix: View the report to see which value was changed. Assure its validity was valid and reset the registry baseline.

{button ,JI(`sysscan.HLP>Main',`Generating_Baseline_Databases')} [More on baseline database](#)

Exploit Not Run

This is an informational message that indicates an exploit was configured to run, but did not due to a dependent exploit not running. This could be due to an error, or mis-configuration of the exploits.

Risk: Low

OS Vulnerable: Windows NT, Windows 9x

Fix: Check the vulnerabilities report for exploit error messages. Be sure that the indicated exploit's dependencies are configured to run.

Max Vulns Logged for this Exploit

Over 100 vulnerabilities have been logged by one Exploit. This is usually due to misconfiguration of the machine or scanner.

Risk: Low

OS Vulnerable: Windows NT, Windows 9x

Fix: Check the vulnerabilities logged by viewing the Vulnerabilities report. This message most likely indicates a change in one of the baseline scans configuration without resetting the baseline.

{button ,JI(`sysscan.HLP>Main',`Generating_Baseline_Databases')}} [More on baseline database](#)

Autologon Password Readable

The autologon password is readable by non-Administrators. If Service Pack 3 has not been applied at the host, attackers can read the autologon password and freely access the system.

Risk: High

OS Vulnerable: Windows NT

Fix: Disable autologon and Apply the latest Windows NT 4.0 Service Pack.

Disable autologon as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.
4. Under **Winlogon**, delete the following values: **AutoAdminLogon** and **DefaultPassword**.

-AND-

[Apply the latest Windows NT 4.0 Service Pack.](#)

Autologon is Enabled

Autologon is enabled. An attacker can access the host as 'DefaultUser,' with the password 'DefaultPassword.'
If the registry is properly secured and the host is properly physically secured, this may not be a threat.

Risk: Low

OS Vulnerable: Windows NT

Fix: Disable autologon and Apply the latest Windows NT 4.0 Service Pack.

Disable autologon as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.
4. Under **Winlogon**, delete the following values: **AutoAdminLogon** and **DefaultPassword**.

-AND-

[Apply the latest Windows NT 4.0 Service Pack.](#)

Windows NT Remote Access Service Running

Remote Access services were discovered. These services provide users dial-in/out capabilities. These services may bypass required security mechanisms and provide network access to attackers.

Risk: Low

OS Vulnerable: Windows NT

Fix: Disable dial-in for remote access services or uninstall the services.

Remove dial-in on Remote Access services as follows:

1. From the **Start** menu, select **Settings, Control Panel, Network**.
2. On the **Services** tab, select one of the Remote Access services.
3. Select **Properties** and click **Configure**.
4. Disable **dial-in**.
5. Repeat for other Remote Access services.

-OR-

Uninstall the services as follows:

1. From the **Start** menu, select **Settings, Control Panel, Services**.
2. Select each of the **Remote Access services** and click the **Stop** button.
3. Also click **Disable** to stop the service from restarting at the next reboot.

SNMP Community Name is World Readable by Default

Windows NT exports information such as valid user names, shares, and the status of running services via SNMP. An attacker can use this information to exploit the computer in a number of ways. The only validation required to read this information is contained in the community name.

Risk: Low

OS Vulnerable: Windows NT

Fix: Edit the registry to permit only approved users access to the SNMP Community Name.

Edit the registry as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities.
4. From the **Security** menu, choose **Permissions**.
5. Set the permissions to permit only approved users access.

HKEY_CLASSES Writeable by Everyone

HKEY_CLASSES_ROOT is writable by everyone. This allows any user to change file associations. If found under NT 4.0, this could be a sign of tampering.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Restrict registry access or reset permissions.

Edit the registry as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_CLASSES_ROOT.
4. From the **Security** menu, choose **Permissions**.
5. Set the permissions to permit only approved users access.

HKEY_LOCAL Writeable by NON-Administrators

HKEY_LOCAL_MACHINE was found to be writable by non-administrator users, allowing these users to change file associations. If found under NT 4.0, this could be a sign of tampering.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Restrict registry access or reset permissions

Edit the registry as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE.
4. From the **Security** menu, choose **Permissions**.
5. Set the permissions to permit only approved users access.

LSA Registry Key Allows Full Access

This vulnerability allows non-administrators write access to a registry key that allows access in plain text to all new passwords. Each time a password is changed or a user is added, these DLLs get called with the userids and plaintext password.

Risk: High

OS Vulnerable: Windows NT

Fix: Set permissions for LSA and/or if the FPNWCLNT.DLL is not used, remove the FPNWCLNT string from the registry.

Set the permissions as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE.
4. From the **Security** menu, choose **Permissions**.
5. Set the permissions to permit only Administrators access.
6. If the FPNWCLNT.DLL is NOT being used, remove the 'FPNWCLNT' string from the **Authentication Packages** value at HKLM/SYSTEM/CurrentControlSet/Control/Lsa/.

Alerter and Messenger Services

The Windows NT Alerter service enables a user to send pop-up messages to other users, which could be used for social engineering attacks. A side effect of running this service is that it causes the name of the current user to be broadcast in the NetBIOS name table, which gives the attacker a valid user name to use in brute force attempts.

Risk: Low

OS Vulnerable: Windows NT

Fix: Disable the Alerter service.

Disable Finger service as follows:

1. From the **Start** menu, choose **Settings, Control Panel, Services**.
2. Under **Services**, select **Alerter**.
3. Click **Stop**.

FPNWCLNT.DLL Has Incorrect Checksum

The FPNWCLNT.DLL was found with an incorrect checksum. An altered DLL may allow access in plain text to all new passwords. Each time a password is changed or a user is added, this DLL gets called with the userids and plaintext password. If an unauthorized security provider has been installed, all accounts on this machine should be considered compromised.

Risk: High

OS Vulnerable: Windows NT

Fix: Apply the latest Windows NT 4.0 Service Pack, convert to NTFS, verify the ACL allows proper access, make sure all values are for password filter packages are legitimate, . Set the permissions properly. If an unauthorized security provider has been installed, and remove FPNWCLNT value or validate the FPNWCLNT.DLL.

[Apply the latest Windows NT 4.0 Service Pack](#)

-AND-

If using FAT system, convert to NTFS as follows:

1. From the **Start** menu, choose **Run**.
2. Type 'cmd' and press **ENTER**. This opens the command prompt.
3. Type **convert c: /fs:ntfs** and press **ENTER**.
4. Reboot your system.
5. Run **chkdsk** to make sure no errors are present.

-AND-

Verify the ACL key as follows:

1. From the **Start** Menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor.
2. Select HKEY_LOCAL_MACHINE.
3. Navigate to SYSTEM/CurrentControlSet/Control/Lsa/
4. From the Security menu, choose 'Permissions'.
5. Verify that the permissions allow write access to Administrators and System.

-AND-

Verify password filter packages as follows:

1. From the Start Menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor.
2. Select HKEY_LOCAL_MACHINE.
3. Navigate to SYSTEM/CurrentControlSet/Control/Lsa/Notification Packages
4. Verify that all values in this key are for password filter packages that Setup intended to install.

-OR-

If you do not use FPNW or DSMN, remove the FPNWCLNT value as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKLM/SYSTEM/CurrentControlSet/Control/Lsa/Authentication Packages.
4. Click **FPNWCLNT** and press **delete**.
5. Verify deletion.

-OR-

If you use FPNW or DSMN, validate the version of FPNWCLNT.DLL is dated 05/01/97 and is size of 35,088.

FPNWCLNT.DLL Incorrect Size

The FPNWCLNT.DLL was found at an incorrect size. An altered DLL may allow access in plain text to all new passwords. Each time a password is changed or a user is added, this DLL gets called with the userids and plaintext password. If an unauthorized security provider has been installed, all accounts on this machine should be considered compromised.

Risk: High

OS Vulnerable: Windows NT

Fix: Apply the latest Windows NT 4.0 Service Pack, convert to NTFS, verify the ACL allows proper access, make sure all values are for password filter packages are legitimate, and set the permissions properly. If an unauthorized security provider has been installed, and remove FPNWCLNT value or validate the FPNWCLNT.DLL.

[Apply the latest Windows NT 4.0 Service Pack](#)

-AND-

If using FAT system, convert to NTFS as follows:

1. From the **Start** menu, choose **Run**.
2. Type 'cmd' and press **ENTER**. This opens the command prompt.
3. Type **convert c: /fs:ntfs** and press **ENTER**.
4. Reboot your system.
5. Run **chkdsk** to make sure no errors are present.

-AND-

Verify the ACL key as follows:

1. From the **Start** Menu, choose 'Run.' Type 'regedt32' and click 'OK.' This opens the Registry Editor.
2. Select HKEY_LOCAL_MACHINE.
3. Navigate to SYSTEM/CurrentControlSet/Control/Lsa/
4. From the Security menu, choose 'Permissions'.
5. Verify that the permissions allow write access to Administrators and System.

-OR-

If you do not use FPNW or DSMN, remove the FPNWCLNT value as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKLM/SYSTEM/CurrentControlSet/Control/Lsa/Authentication Packages.
4. Click **FPNWCLNT** and press **delete**.
5. Verify deletion.

-OR-

If you use FPNW or DSMN:

1. Validate the version of FPNWCLNT.DLL is dated 05/01/97 and is size of 35,088.

FPNWCLNT DLL Was Not Found

This file could be added to enable access in plain text to all new passwords. Each time a password is changed or a user is added, this DLL gets called with the userids and plaintext password.

Risk: High

OS Vulnerable: Windows NT

Fix: If you do not use FPNW or DSMN, remove the FPNWCLNT value from the registry.

If you do not use FPNW or DSMN, remove the FPNWCLNT value as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to SYSTEM/CurrentControlSet/Control/Lsa/Notification Packages.
4. Click **FPNWCLNT** and press **delete**.
5. Verify deletion.

Windows NT Messenger Service Running

The Windows NT Messenger service enables a user to send pop-up messages to other users, which could be used for social engineering attacks. A side effect of running this service is that it causes the name of the current user to be broadcast in the NetBIOS name table, which gives the attacker a valid user name to use in Brute Force attempts.

Risk: Low

OS Vulnerable: Windows NT

Fix: Disable the Messenger service.

Disable the Messenger service as follows:

1. From the **Start** menu, choose **Settings, Control Panel, Services**.
2. Under **Services**, select **Messenger**.
3. Click **Stop**.

LSA Registry Key Altered

This system was found with an altered LSA registry key. This may allow access in plain text to all new passwords. Each time a password is changed or a user is added, these DLLs get called with the userids and plaintext password. If an unauthorized security provider has been installed, all accounts on this machine should be considered compromised.

Risk: High

OS Vulnerable: Windows NT

Fix: Set the permissions properly or remove the FPNWCLNT.DLL.

Set the permissions for the ACL key as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to SYSTEM/CurrentControlSet/Control/Lsa/.
4. From the **Security** menu, choose **Permissions**.
5. Verify that the permissions allow write access to Administrators and System.

-OR-

If you do not use FPNW or DSMN, remove the FPNWCLNT value as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKLM/SYSTEM/CurrentControlSet/Control/Lsa/Authentication Packages.
4. Click **FPNWCLNT** and press **delete**.
5. Verify deletion.

Windows NT Rlogin Service Installed

The Windows NT machine is running the Ataman rlogin service. A user with an rlogin client could potentially compromise the machine's security with a brute force password attack. Also, this service could potentially write sensitive information to the NT Application Log.

Risk: Low

OS Vulnerable: Windows NT

Fix: Check the user password or disable the **Ataman rlogin** service.

Check the user password as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select **User**.
3. From the **Policies** menu, choose **Account**.
4. Set the password values in accordance with your security policy.
5. Click **OK**.

-OR-

*Disable **Ataman rlogin** service as follows:*

1. From the **Start** menu, choose **Settings, Control Panel, Services**.
2. Under **Services**, select **FTP**.
3. Click **Stop**.

Performance Monitor Readable

The permissions on the Software\Microsoft\Windows NT\CurrentVersion\Perflib key are incorrect. This allows non-administrators to read performance counters, and monitor which processes are running. Under NT 4.0, registry access from the network can be denied completely.

Risk: Low

OS Vulnerable: Windows NT

Fix: Restrict registry access and/or reset permissions.

Restrict registry access as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Perflib.
4. From the **Security** menu, choose **Permissions**.
5. Verify that the permissions allow write access to Administrators and System.

Windows NT Rcmd Service Running

The Rcmd service was found running. This service allows users to execute command line programs from remote hosts. It is distributed in the Windows NT Resource Kit, and uses native Windows NT challenge-response authentication. Due to the fact it uses encrypted authentication and not host level authentication, it is not known to be vulnerable to spoofing.

Risk: Low

OS Vulnerable: Windows NT

Fix: Remove the rcmd service.

Remove the rcmd service as follows:

1. From the **Start** menu, choose **Settings, Control Panel, Services**.
2. Under **Services**, select **rcmd**.
3. Click **Stop**.

Windows NT Registry Opened Remotely

This indicates that the Scanner is able to open the registry remotely. This may indicate that permissions are not set properly, or that possibly the guest account is enabled with network access rights. An attacker could alter file associations, permitting the introduction of a [trojan horse](#), or otherwise seriously compromise the machine. If the host running the scan is a trusted host, this may not indicate a vulnerability. Under NT 4.0, registry access from the network can be denied completely

Risk: Low

OS Vulnerable: Windows NT

Fix: Restrict registry access and/or reset permissions.

Restrict registry access as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg.
4. From the **Security** menu, choose **Permissions**.
5. Restrict access to all or set permissions to allow access to approved Administrators only.

Windows NT Rexec Service Running

The rexec service has been found. This service allows a user to execute commands remotely, and typically requires that user names and passwords be passed in clear text across the network. Under Windows NT, the Ataman version of this service writes errors to the application log. The application log is readable by any user with permission to access the computer from the network, which could potentially report details about why a given user was unable to log in.

Risk: Low

OS Vulnerable: Any

Fix: Remove the rexec service.

Disable the rexec service as follows:

1. From the **Start** menu, choose **Settings, Control Panel, Services**.
2. Under **Services**, select **rexec**.
3. Click **Stop**.

Windows NT Rsh Service Running

The Rsh service was detected. A version of rsh ships with the Windows NT Resource Kit which executes all commands, regardless of user, under the system account. The system account is the most powerful account on a Windows NT computer, and it is not recommended that this service be run under any circumstances. The instsrv tool, which also ships with the Windows NT Resource Kit, can be used to remove the rsh service.

Risk: High

OS Vulnerable: Windows NT

Fix: Remove the rshsvc service.

Disable the service as follows:

1. From the **Start** menu, choose **Settings, Control Panel, Services**.
2. Under **Services**, select **rshsvc**.
3. Click **Stop**.

Windows NT Schedule Service Running

The Windows NT schedule service was detected. This service allows administrators to schedule batch jobs to occur at specified times. Since the schedule service normally executes jobs as the system account, it can be used to modify account privileges. It is also disabled as part of the configuration needed to make a Windows NT machine C2 secure. Due to the fact that the schedule service requires administrator level access to cause jobs to run, it is considered a low risk.

Risk: Low

OS Vulnerable: Windows NT

Fix: Remove the schedule service.

Disable the service as follows:

1. From the **Start** menu, choose **Settings, Control Panel, Services**.
2. Under **Services**, select **schedule**.
3. Click **Stop**.

Windows NT Telnet Service Installed

The Windows NT machine is running the Ataman telnet service. A user with a telnet client could potentially compromise the machine's security with a Brute Force password attack. Also, this service could potentially write sensitive information to the NT Application Log.

Risk: Low

OS Vulnerable: Windows NT

Fix: Check user passwords or disable *the ataman service*.

Check the user password as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select **User**.
3. From the **Policies** menu, choose **Account**.
4. Set the password values in accordance with your security policy.
5. Click **OK**.

Disable the service as follows:

1. From the **Start** menu, choose **Settings, Control Panel, Services**.
2. Under **Services**, select **ataman**.
3. Click **Stop**.

Registry Access Allowed For All Users

The winreg key was found to be vulnerable. The permissions on the SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg key control remote access to the registry. If the 'everyone' group is not allowed access, null session access to the registry can be prevented. If this key is not present, remote access to the registry is not controlled, and if found in conjunction with Service Pack 3 not applied, can allow non-authenticated users to write registry keys.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Apply the latest Windows NT 4.0 Service Pack and modify the registry for RestrictAnonymous.

[Apply the latest Windows NT 4.0 Service Pack](#)

-AND-

Restrict registry access as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\SecurePipeServers\Winreg.
4. From the **Security** menu, choose **Permissions**.
5. Restrict access **Everyone**.

Registry Access Unrestricted From Network

The SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg key is not present. This key controls remote access to the registry. If the 'everyone' group is not allowed access, null session access to the registry can be prevented. If this key is not present, remote access to the registry is not controlled, and if found in conjunction with Service Pack 3 not applied, can allow non-authenticated users to write registry keys.

Risk: High

OS Vulnerable: Windows NT

Fix: Apply the latest Windows NT 4.0 Service Pack and modify the registry for RestrictAnonymous.

[Apply the latest Windows NT 4.0 Service Pack](#)

-AND-

Set permission to the winreg key in the NT registry as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA.
4. From the **Security** menu, choose **Permissions**.
5. Restrict access from **Everyone**.

Windows Key with Incorrect Permissions

The HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion key is set to allow any user to modify the subkeys. This allows members of the "Everyone" group to create an entry under the Run and RunOnce keys that contains the name of a program to run when the computer starts.

Risk: High

OS Vulnerable: Windows NT

Fix: Set the registry permissions to allow read access to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion.

Set permissions as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion.
4. From the **Security** menu, choose **Permissions**.
5. Allow only read access to the **Everyone** group.

DCOM Can Be Enabled By Non-Admins

Permissions were found improperly set for the DCOM registry key. If enabled, DCOM may be used to execute programs remotely.

Risk: Low

OS Vulnerable: Windows NT

Fix: Restrict non-administrators write access to the Ole key in the NT registry.

Set registry permissions as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Ole.
4. From the **Security** menu, choose **Permissions**.
5. Restrict non-Administrators write access.

DCOM is Enabled.

DCOM was found to be enabled. DCOM may be used to execute programs remotely.

Risk: Low

OS Vulnerable: Windows NT

Fix: Disable DCOM in the NT registry.

Disable DCOM as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Ole.
4. Open the **EnableDCOM** key and change the value to **N**.
5. Click **OK**.

Regfile Associations Can Be Changed By Non-Admins

Improper permissions were found on the registry key valuenam specifying a command association with registry files.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Restrict non-Administrators write access for the command key in the NT registry.

Restrict access as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE/Software/Classes/regfile/shell/open/command.
4. From the **Security** menu, choose **Permissions**.
5. Restrict non-Administrators write access.

Regedit is Associated with .reg files

Regedit.exe was found associated with registry files.

Risk: Medium

OS Vulnerable: Windows NT, Windows 9x

Fix: Associate the .reg file name extension with a text editor:

Windows NT: Change the association from the File Types dialog:

1. Open My Computer.
2. From the **View** menu, select **Folder Options**.
3. Select the **File Types** tab.
4. In the registered file types list, locate and select **Registration Entries**.
5. Click **Edit**.
6. In the **Actions** list, click the first action.
7. Click **Edit**.
8. Change all references of regedit.exe to a text editor, such as notepad.exe or wordpad.exe and click **OK**.
9. Repeat steps 6 through 8 for each action in the **Actions** list.
10. Click **OK**, then click **Close** twice to apply the changes.

Windows 95: Because of a problem with existing associations reverting when set from the File Types dialog, remove and add the association, or change the association from the registry.

1. Open the Registry Editor.
 2. Go to the **HKEY_LOCAL_MACHINE/Software/Classes/regfile/shell/open/command key**.
 3. Double click the value that is similar to <No Name> : REG_SZ : regedit.exe %1. The String Editor window appears.
 4. Change the regedit.exe entry to notepad.exe. Do not alter any other portion of the string.
 5. Click **OK**.
- See the references for more information.

WARNING: Incorrectly using Registry Editor may cause severe and irreparable damage and may require you to reinstall your operating system. Internet Security Systems cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

--AND--

Set appropriate registry permissions to prevent non-administrators from changing the HKEY_LOCAL_MACHINE/SOFTWARE/Classes/regfile/shell/open/command key or its values.

After completing the association, if a .reg file appears in your text editor, then an attack may be in progress to compromise your system.

References:

Microsoft Knowledge Base article Q132664 "Changing Association in File Types Dialog Box May Not Work" at <http://support.microsoft.com/support/kb/articles/q132/6/64.asp> .

Winlogon Key Has Incorrect Permissions

The HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon key has two values which can be used to cause a process to execute upon either system bootup, or when a user logs on. The programs pointed to by the System value run under the system user context after boot, and could be used to change a user's rights or access level. The UserInit value runs applications when a user logs in. The default settings for this key allow Server Operators to write these values, either of which could be used to raise a System Operator's access level to Administrator.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Remove Server Operator write access to the winlogon key.

Remove association as follows as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.
4. From the **Security** menu, choose **Permissions**.
5. Remove Server Operator write access.

Scheduler Key Has Incorrect Permissions

The HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Schedule key controls the schedule service. Server Operators have permission to write to this registry tree, which would allow them to manually schedule jobs to be run by the schedule service, which normally executes under the system user context. This can be used to raise the Server Operator's access level to Administrator.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Remove Server operator write access to the schedule key in the NT registry.

Remove write access as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Schedule.
4. From the **Security** menu, choose **Permissions**.
5. Remove Server Operator write access.

Multihomed Host

The Scanner has detected that the host has more than one network card installed. Under ordinary circumstances, this is not considered a serious risk. If the host is placed outside the firewall, it could provide an entry point for an intruder. Note - this vulnerability was determined by reading the Windows NT registry.

Risk: Low

OS Vulnerable: Windows NT

Fix: If multihomed hosts are outside of your security policy, remove the additional network adapter.

Multiple Protocols Active

The Scanner has detected that the host has more than one protocol active. If the host is outside a firewall, it could provide an entry point for an intruder into the internal network.

Risk: Low

OS Vulnerable: Windows NT

Fix: If multiple protocols are not allowed by your security policy, remove the protocols not in use.

Remove unused protocols as follows:

1. From the **Start** menu, choose **Settings, Control Panel**.
2. Open the **Network** icon.
3. Click the **Protocols** tab.
4. Remove unwanted protocols.
5. Click **OK**.
6. Reboot the system to allow this change to take effect.

For more information, consult your firewall documentation.

DCOM RunAs Value Altered

The DCOM RunAs Value was found to be altered. DCOM calls are executed under the security context of the calling user by default. If the RunAs key has been altered, the DCOM calls can be executed under the user context of the currently logged in user, or as a third user. If this ability is not controlled very carefully, it could provide a network user with the ability to execute arbitrary code under another user context.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Remove the RunAs value to restore the user context to that of the calling user.

Remove the RunAs value as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE\Software\Classes\AppID.
4. Locate the subkey which has had the **RunAs** value inserted.
5. Remove the **RunAs** value.

DCOM RunAs Value Writeable

The DCOM RunAs Value was found to be writable. DCOM calls are executed under the security context of the calling user by default. If the RunAs key has been altered, the DCOM calls can be executed under the user context of the currently logged in user, or as a third user. If this ability is not controlled very carefully, it could provide a network user with the ability to execute arbitrary code under another user context. The RunAs key is writable by the Interactive (console) user by default, which implies that if the console user were tricked into executing a trojan which altered the registry, or if someone other than the normal user were to log on locally, then DCOM calls could be executed under the console user's context by a remote user. If the console user was of a higher access level than the network user, a security breach could result.

Risk: Low

OS Vulnerable: Windows NT

Fix: Remove Interactive User write access to the AppID Key in the NT registry.

Remove write access as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKEY_LOCAL_MACHINE\Software\Classes\AppID.
4. From the **Security** menu, choose **Permissions**.
5. Remove Interactive user write permissions and propagate these permissions down that portion of the registry tree.

IP Forwarding Enabled

The host has IP forwarding enabled. If this machine is outside of the firewall, this could allow access to internal networks.

Risk: Low

OS Vulnerable: Windows NT

Fix: If IP forwarding is NOT allowed by your security policy, disable IP forwarding.

Locally:

1. From the **Start** menu, choose **Settings, Control Panel**.
2. Open the **Network** icon.
3. Click the **Protocols** tab, and select the protocol in use.
4. Click **Properties**.
5. Click the **Routing** tab, and disable the **Enable IP Forwarding** checkbox.
6. Click **OK**.
7. Click **OK**.
8. Reboot the system to allow this change to take effect.

Remotely:

1. Open the registry on the remote host.
2. Navigate to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters.
3. Set the **IPEnableRouter** value to zero.
4. Reboot the system to allow this change to take effect.

NetBIOS Information Available From SNMP

By default, Windows NT provides information which is normally available only to administrators via SNMP. If your security policy does not allow publishing information about Windows NT services, users, and shares via a protocol with very minimal security, disable SNMP or this feature.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Remove a value that contains SOFTWARE\Microsoft\LANManagerMIB2Agent\CurrentVersion to restore the user context to that of the calling user.

Remove the value as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to **HKLM\System\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents**.
4. Locate the value which contains **SOFTWARE\Microsoft\LANManagerMIB2Agent\CurrentVersion** and remove it.

Page File Not Cleared at Shutdown

The Windows NT pagefile can contain sensitive information, and should be cleared upon shutdown if required by your security policy. Some versions of the Netware authentication module will store the user name and password in clear-text, and this can be extracted from the pagefile.

Risk: Low

OS Vulnerable: Windows NT

Fix: Activate the ClearPageFileAtShutdown value.

Activate the ClearPageFileAtShutdown value as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HKLM\System\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents.
4. Locate the 'ClearPageFileAtShutdown' value, and set it to 1.

Posix Enabled

Windows NT was C2 evaluated with the POSIX subsystem disabled. Enabling the POSIX subsystem can also subject a host to [trojan horse](#) attacks, since it is possible to create a file with a lower case name which will be found in a search prior to a file with an upper case name.

Risk: Low

OS Vulnerable: Windows NT

Fix: Remove the POSIX value.

Remove the POSIX value as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HSystem\CurrentControlSet\Control\Session Manager\SubSystems.
4. Remove the POSIX value, and the file which is pointed to be the value data.

OS/2 Subsystem Enabled

Windows NT was C2 evaluated with the OS/2 subsystem disabled. Enabling the OS/2 subsystem can allow a process to persist across logins.

Risk: Low

OS Vulnerable: Windows NT

Fix: Remove the Os2 value from the NT registry.

Remove the Os2 value as follows:

1. From the **Start** menu, choose **Run**.
2. Type **regedt32** and click **OK**. This opens the Registry Editor.
3. Navigate to HSystem\CurrentControlSet\Control\Session Manager\SubSystems.
4. Remove the Os2 value, and the file which is pointed to be the value data.

Incorrect Passfilt.dll Found

An unknown version of passfilt.dll was found. Passfilt.dll was distributed by Microsoft for Service Pack 2 and above and rejects weak passwords. The version of Passfilt.dll which was found differs either in size or checksum from the known versions distributed by Microsoft, and could be a [trojan horse](#).

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the version of passfilt.dll which is installed is correct and has not been tampered with.

System Auditing not Enabled

System Event Auditing is not enabled. System events include startup and shutdown.

Risk: Low

OS Vulnerable: Windows NT

Fix: Enable Restart, Shutdown, and System auditing.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, choose **Audit**.
4. Enable **Restart, Shutdown, and System** auditing on **Success** and **Failure**.

Logon Auditing Not Enabled

Logon Auditing is not enabled. It is important to audit logon and logoff success and failure to be able to detect and track unauthorized access attempts.

Risk: Low

OS Vulnerable: Windows NT

Fix: Enable Logon and Logoff auditing.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, choose **Audit**.
4. Enable **Logon and Logoff** auditing on **Success** and **Failure**.

Object Auditing Not Enabled

Object Auditing is not enabled. Object access includes files and registry keys. Auditing of these events must be enabled both by the security descriptor on the object and in the auditing settings.

Risk: Low

OS Vulnerable: Windows NT

Fix: Enable File and Object Access auditing.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, choose **Audit**.
4. Enable **File and Object Access** auditing on **Success** and **Failure**.

Privilege Auditing Not Enabled

Privilege Auditing is not enabled. Privilege auditing records when any user rights (such as the right to backup and restore files) are granted to a user or process.

Risk: Low

OS Vulnerable: Windows NT

Fix: Enable Use of User Rights auditing.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, choose **Audit**.
4. Enable **Use of User Rights** auditing on **Success** and **Failure**.

Process Auditing Not Enabled

Process Auditing is not enabled. Process auditing records when processes are started and stopped. Auditing these events typically produces a large number of event logs, and is not normally enabled.

Risk: Low

OS Vulnerable: Windows NT

Fix: Enable Process Tracking auditing.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, choose **Audit**.
4. Enable **Process Tracking** auditing on **Success** and **Failure**.

Policy Auditing Not Enabled

Policy Auditing is not enabled. Policy auditing records when security policy changes are made. Since these events are highly sensitive, it is recommended that these events always be audited.

Risk: Low

OS Vulnerable: Windows NT

Fix: Enable Security Policy Changes auditing.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, choose **Audit**.
4. Enable **Security Policy Changes** auditing on **Success** and **Failure**.

Account Management Auditing Not Enabled

Account Management Auditing is not enabled. Account Management auditing records when new users and groups are created or changed. Since these events are highly sensitive, it is recommended that these events always be audited.

Risk: Low

OS Vulnerable: Windows NT

Fix: Enable User and Group Management auditing.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, choose **Audit**.
4. Enable **User and Group Management** auditing on **Success** and **Failure**.

Inappropriate User with Create Token Name Privilege

A user has been detected with Create Token Name privileges. This right is not normally granted to any users.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Create a Token Object**.
5. Verify that this is not granted to any users.

Inappropriate User with Replace Process Token Privilege

A user has been found with Replace Process Token privileges. This right is not normally granted to any users, and can be used to attain administrative rights.

Risk: High

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Create a process level token**.
5. Verify that this is not granted to any users.

Inappropriate User with Lock Memory Privilege

A user has been found with Lock Memory privileges. This right is not normally granted to any users.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Lock pages in memory**.
5. Verify that this is not granted to any users.

Inappropriate User with Increase Quota Privilege

A user has been found with Increase Quota privileges. This right is not normally granted to any users. It is currently unused by Windows NT.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **increase quotas**.
5. Verify that this is not granted to any users.

Inappropriate User with Unsolicited Input Privilege

A user has been found with Unsolicited Input privileges. This right is not normally granted to any users.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **unsolicited input**.
5. Verify that this is not granted to any users.

Inappropriate User with Act as System Privilege

A user has been detected with Act as System privileges. This right is not normally granted to any users, and can be used to attain administrative rights.

Risk: High

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Act as part of the operating system**.
5. Verify that this is not granted to any users.

Inappropriate User with Create Permanent Object Privilege

A user has been detected with Create Permanent Object privileges. This right is not normally granted to any users, and can be used to attain administrative rights.

Risk: High

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Create permanent shared objects**.
5. Verify that this is not granted to any users.

Inappropriate User with Generate Security Audit Privilege

A user has been found with Generate Security Audit privileges. This right is not normally granted to any users.

Risk: High

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Generate Security Audits**.
5. Verify that this is not granted to any users.

Inappropriate User with Add Workstation Privilege

A user has been found with Add Workstation privileges. This right is normally granted to only Domain Administrators.

Risk: High

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Add workstations to domains**.
5. Verify that this is not granted to any users.

Inappropriate User with Manage Security Log Privilege

A user has been found with Manage Security Log privileges. This right is normally granted to only Administrators.

Risk: High

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Manage auditing and security log**.
5. Verify that this is not granted to any users.

Inappropriate User with Take Ownership Privilege

A user has been found with Take Ownership privileges. This right is normally granted to only Administrators.

Risk: High

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Take ownership of files or other objects**.
5. Verify that this is not granted to any users.

Inappropriate User with Load Driver Privilege

A user has been found with Load Driver privileges. This right is normally granted to only Administrators.

Risk: High

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Load and unload device drivers**.
5. Verify that this is not granted to any users.

Inappropriate User with Profile System Privilege

A user has been found with Profile System privileges. This right is normally granted to only Administrators.

Risk: High

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Profile System Performance**.
5. Verify that this is not granted to any users.

Inappropriate User with Change System Time Privilege

A user has been found with Change System Time privileges. This right is normally granted to only Administrators and Power Users.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Change the system time**.
5. Verify that this is not granted to any users.

Inappropriate User with Profile Single Process Privilege

A user has been found with Profile Single Process privileges. This right is normally granted to only Administrators and Power Users.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Profile single process**.
5. Verify that this is not granted to any users.

Inappropriate User with Increase Priority Privilege

A user has been found with Increase Priority privileges. This right is normally granted to only Administrators and Power Users.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Increase scheduling priority**.
5. Verify that this is not granted to any users.

Inappropriate User with Create Pagefile Privilege

A user has been detected with Create Pagefile privileges. This right is normally granted to only Administrators.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Create a pagefile**.
5. Verify that this is not granted to any users.

Inappropriate User with Backup Privilege

A user has been found with Backup privileges. This right is normally granted to only Administrators and Backup operators, and can be used to read any file or registry key, regardless of permissions. If the user also has restore privileges, the ownership of files and other objects can be changed.

Risk: High

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Backup Files and Directories**.
5. Verify that this is not granted to any users.

Inappropriate User with Restore Privilege

A user has been found with Restore privileges. This right is normally granted to only Administrators and Backup operators, and can be used to replace any file or registry key, regardless of permissions. If the user also has backup privileges, the ownership of files and other objects can be changed.

Risk: High

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Restore Files and Directories**.
5. Verify that this is not granted to any users.

Inappropriate User with Debug Privilege

A user has been detected with Debug privileges. This right is normally granted to only Administrators, and can be used to obtain higher access levels. Under some circumstances, it may be best not to grant this right to any user.

Risk: High

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Debug Programs**.
5. Verify that this is not granted to any users.

Inappropriate User with System Environment Privilege

A user has been found with System Environment privileges. This right is normally granted to only Administrators, and can be used to obtain higher access levels.

Risk: High

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Modify firmware environment values**.
5. Verify that this is not granted to any users.

Inappropriate User with Remote Shutdown Privilege

A user has been found with Remote Shutdown privileges. This right is normally granted to only Administrators and Power Users.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify Advanced user rights in User Manager.

Enable auditing as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Enable the **Show Advanced User Rights** checkbox.
4. Under **Right**, select **Force shutdown from a remote system**.
5. Verify that this is not granted to any users.

GetAdmin Present on Host

The getadmin exploit has been run on this host. Problems in Windows NT kernel functions allowed a flag to be set inside the operating system which allows any user to gain administrator privileges. Getadmin leaves a Software\AntiShut key in the registry, and this key has been detected. An early work-around to getadmin developed by ISS was to create that key and deny non-administrators access, so if this key is present but is not writable by non-admins, it is considered not to be a vulnerability.

Risk: High

OS Vulnerable: Windows NT

Fix: Verify that your system is compromised by checking for users with administration rights. If there are not any users with administrator rights then fix the kernel by applying the getadmin-fix. If users are present with administrator rights, re-install Windows NT and install the getadmin-fix.

Verify your system as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. From the **Policies** menu, choose **User Rights**.
3. Check if users have admin privileges on that host.

Apply getadmin fix as follows:

1. From the **Start** menu, choose **Run**.
2. Type ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/getadmin_-fix and press **ENTER**.
3. View the README.TXT for patch version and execution.

NetBIOS Share Found

This vulnerability indicates that a NetBIOS share has been found. If the share has the proper access controls, this is a medium risk vulnerability.

Risk: Low

OS Vulnerable: Windows NT, Windows 9x, OS/2, Unix Samba, Windows for Workgroups 3.11

Fix: Correct the share permissions or remove the share.

LOCAL MACHINE:

Set the permissions explicitly as follows:

1. Navigate to the share in Windows Explorer.
2. Right-click the share, select **Properties**.
3. Under the **Sharing** tab, review the permissions.
4. Allow access only to approved users.
5. Click **OK**.

-OR-

Open the command line, remove the share as follows:

1. From the **Start** menu, select **Run**.
2. Type **cmd**, then click **OK**. This opens the command line.
3. Type **net share sharename /delete**, where sharename is the name of the share.
4. Type **exit** to return to the Windows NT desktop.

REMOTE HOST (GUI):

Remove the share as follows:

1. From the **Start** menu, select **Programs, Administrative Tools (Common), Server Manager**.
2. Select the host. From the **Computer** menu, select **Shared Directories**.
3. Select the share and click **Stop Sharing**.

NetBIOS Share Has No Access Control

A NetBIOS share was found with no access control list. The absence of an access control list permits attackers to access the shared resource (drive).

Risk: Medium

OS Vulnerable: Windows NT

Fix: Correct the share permissions or remove the share.

LOCAL MACHINE:

Set the permissions explicitly as follows:

1. Navigate to the share in Windows Explorer.
2. Right-click the share, select **Properties**.
3. Under the **Sharing** tab, review the permissions.
4. Allow access only to approved users.
5. Click **OK**.

-OR-

Open the command line, remove the share as follows:

1. From the **Start** menu, select **Run**.
2. Type **cmd**, then click **OK**. This opens the command line.
3. Type **net share sharename /delete**, where sharename is the name of the share.
4. Type **exit** to return to the Windows NT desktop.

REMOTE HOST (GUI):

Remove the share as follows:

1. From the **Start** menu, select **Programs, Administrative Tools (Common), Server Manager**.
2. Select the host. From the **Computer** menu, select **Shared Directories**.
3. Select the share and click **Stop Sharing**.

Windows NT Network Monitor

NetMon has a weakly decrypted password in a DLL. Access to this would allow an attacker to gain access to the network monitor.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Disable the Network Monitor Agent and remove the BHSUPP.DLL from %systemroot%\system32. If the Network Monitor is required, use a unique password.

Disable the Network Monitor agent as follows:

1. From the 'Start' menu, select 'Settings', 'Control Panel', 'Services'.
2. Select the Network Monitor service and click 'Stop.'

-AND-

Remove BHSUPP.DLL from %systemroot%\system32.

Unknown NT Service

A service was found which was not known to ship with Windows NT. Services can be used to install back doors, or provide unauthorized network access. Any service which is not approved by your security policy should be removed.

Risk: Low

OS Vulnerable: Windows NT

Fix: Use **instsrv** from the Windows NT Resource Kit to remove the unwanted service.

Remove the service as follows:

1. From the **Start** menu, choose **Run**.
2. Type **cmd** and click **OK**. This opens the command line.
3. At a command prompt, type **instsrv [service name] remove** and press **<ENTER>**.
4. Type **exit** and press **<ENTER>** to return to windows.

File permissions changed since baseline scan

The permissions for the file have changed since the file baseline scan was run.

Risk: High

OS Vulnerable: Windows NT

Fix: Check the current permissions to make sure they are appropriate.

Verify security permissions as follows:

1. In Explorer, right click the file with changed permissions.
2. Click **Properties**.
3. Under the **Security** tab, click the **Permissions** button.
4. Check the permissions and change as necessary.

File owner changed since baseline scan

Since the last file baseline scan, the owner for the file has changed.

Risk: High

OS Vulnerable: Windows NT

Fix: Check the current owner of the file to make sure an unauthorized user has reset the ownership.

Verify security permissions as follows:

1. In explorer, right click the file with the changed ownership.
2. Click **Properties**.
3. Under the **Security** tab, click the **Ownership** button.
4. Verify proper ownership or take ownership by clicking the **take ownership** button.

Registry key permissions changed since baseline scan

The permissions for the key have changed since the registry baseline scan was run.

Risk: High

OS Vulnerable: Windows NT

Fix: Check the current permissions to make sure they are appropriate.

Check registry key permissions as follows:

1. From the **Start** menu, Click **Run**.
2. Type **regedt32** and press enter. This opens the NT registry editor.
3. Navigate to the directory for the key with changed permissions.
4. From the **Security** menu, choose **Permissions**.
5. Verify proper permissions for the key.

Registry key owner changed since baseline scan

Since the last registry baseline scan, the owner for the key has changed.

Risk: High

OS Vulnerable: Windows NT

Fix: Check the current owner of the key to make sure an unauthorized user has reset the ownership.

Check registry key ownership as follows:

1. From the **Start** menu, Click **Run**.
2. Type **regedt32** and press enter. This opens the NT registry editor.
3. Navigate to the directory for the key with changed ownership.
4. From the **Security** menu, choose **Owner**.
5. Verify proper ownership for the key.

File attributes changed since baseline scan

The attributes for the file have changed since the file baseline scan.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Check the current attributes to make sure they are appropriate. The scanner checks read-only, system, and encrypted attributes. Changing these may impact the performance of the system or an application.

Verify security permissions as follows:

1. In Explorer, right click the file with changed attributes.
2. Click **Properties**.
3. Under the **General** tab, verify proper attributes.

Folder attributes changed since baseline scan

The attributes for the folder have changed since the file baseline scan was run.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Check the current attributes to make sure they are appropriate. The scanner checks read-only, system, and encrypted attributes. Changing these may impact the performance of the system or an application.

Verify security permissions as follows:

1. In Explorer, right click the directory with changed attributes.
2. Click **Properties**.
3. Under the **General** tab, verify proper attributes.

Folder permissions changed since baseline scan

Since the last folder baseline scan, the permissions for the folder have changed.

Risk: High

OS Vulnerable: Windows NT

Fix: Check the current permissions to make sure they are appropriate.

Verify security permissions as follows:

1. In Explorer, right click the folder with changed permissions.
2. Click **Properties**.
3. Under the **Security** tab, click the **Permissions** button.
4. Check the permissions and change as necessary.

Folder owner changed since baseline scan

Since the last folder baseline scan, the owner for the folder has changed.

Risk: High

OS Vulnerable: Windows NT

Fix: Check the current permissions to make sure they are appropriate.

Verify security permissions as follows:

1. In Explorer, right click the folder with the changed owner.
2. Click **Properties**.
3. Under the **Security** tab, click the **Ownership** button.
4. Verify proper ownership or take ownership by clicking the **take ownership** button.

Folder added since baseline scan

A folder was added since the baseline scan was run. This new folder could be a normal folder, or evil and malicious.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Check to see when this folder was added and what software added it.

If it is confirmed as safe, re-run the baseline scan.

File deleted since baseline scan

A file was deleted since the baseline scan was run.

Risk: Low

OS Vulnerable: Windows NT, Windows 95

Fix: Check to see if the file was a critical one and restore or re-install it.

Folder deleted since baseline scan

A folder was deleted after running a baseline scan.

Risk: Low

OS Vulnerable: Windows NT, Windows 95

Fix: Check to see if the folder was a critical one and restore or re-install it.

Folder audit settings changed since baseline scan

Since running the last folder baseline scan, the audit settings for the folder have changed.

Risk: High

OS Vulnerable: Windows NT

Fix: Check to see if the folder was a critical one and restore or re-install it.

Check auditing as follows:

1. In Explorer, right click the folder with changed auditing.
2. Click **Properties**.
3. Under the **Security** tab, click the **Auditing** button.
4. Check the auditing settings and change as necessary.

File Audit settings changed since baseline scan

Since running the last file baseline scan, the audit settings for the file have changed.

Risk: High

OS Vulnerable: Windows NT

Fix: Check to see if the folder was a critical one and restore or re-install it.

Check auditing as follows:

1. In Explorer, right click the file with changed auditing.
2. Click **Properties**.
3. Under the **Security** tab, click the **Auditing** button.
4. Check the auditing settings and change as necessary.

Registry key audit settings changed since baseline scan

Since running the last registry baseline scan, the audit settings for the key have changed.

Risk: High

OS Vulnerable: Windows NT

Fix: Check the current settings to see if dangerous actions on the key are no longer audited.

Check registry key auditing as follows:

1. From the **Start** menu, Click **Run**.
2. Type **regedt32** and press enter. This opens the NT registry editor.
3. Navigate to the directory for the key with changed auditing.
4. From the **Security** menu, choose **Auditing**.
5. Verify proper auditing settings for the key.

User baseline was reset

This is to inform the operator that someone has reset the baseline user scan on their machine. This is a potential vulnerability. If the baseline is reset after a [trojan horse](#) is installed, the trojan horse will go undetected.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the baseline was legitimately reset. This means that you know who reset it or why it was reset.

User added since baseline scan

Since running the last user baseline scan, a new user was added.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify that the new user was legitimately added.

Validate the user as follows:

1. From the **Start** menu, select **Programs, Administrative Tools (Common), User Manager**.
2. Highlight the new user, from the **Policies** menu, choose **User Rights**.
3. Under the **Sharing** tab, review the permissions.
4. Allow access only to approved users.
5. Click **OK**.

User deleted since baseline scan

A user was deleted since the user baseline scan was run. Aside from preventing logons, deleting users may cause problem for services or DCOM applications.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that deleting the user was legitimate. You should know who deleted the user or why the user was deleted.

User logon changed since user baseline scan

A user's logon information has changed since the user baseline scan was run. Logon information includes:

- Home Directory Local Path
- Connect To
- Logon Script Name
- User Profile Path

Risk: Low

OS Vulnerable: Windows NT

Fix: Make sure the user's logon information is setup correctly for your installation. Removing logon information may allow users to access more of the machine than the administrator desires.

Verify user logon setup as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **User** menu, choose **Properties**.
4. At the bottom of the screen, click the **Profile** button.
5. Assure the profile information is correct.

User dial-in settings changed since baseline scan

The user's dial-in settings have changed since the user baseline scan was run. This could be their Dialin access or call back phone number.

Risk: High

OS Vulnerable: Windows NT

Fix: Make sure the user's Dialing settings are setup correctly for your installation. Changing these settings could allow a remote user access to the machine.

Verify user dialin settings as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **User** menu, choose **Properties**.
4. At the bottom of the screen, click the **Dialin** button.
5. Assure the dialin information is correct.

User rights changed since baseline scan

The user's rights have changed since the user baseline scan was run. This could allow users access to critical OS features.

Risk: High

OS Vulnerable: Windows NT

Fix: Check the user's rights to make sure they are correct.

Verify user rights as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **Policies** menu, choose **User's Rights**.
4. Assure the rights are granted to appropriate users.

User group membership changed since baseline scan

A user's group membership has changed since the user baseline scan was run. This could change the access for the user.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Check the user's group to make sure they are correct..

Verify user groups as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Select the account.
3. From the **User** menu, choose **Properties**.
4. At the bottom of the screen, click the **Groups** button.
5. Assure the user is a member of the appropriate groups.

A user has Dialin permission

A user has dialin permission. This means the user may access the machine remotely.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Check with your administrator to see if the user should have *dialin* permissions.

A user has can change callback number

A user has permission to change the callback telephone number for Dialin access. This allows the user to change locations for Dialin access.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Check with your administrator to see if the user should have *call back* permissions.

A user's password never expires

A user's password never expires. If there is no expiration, and the password is cracked, it is never changed. This is a risk because it allows unauthorized access to appear as authorized access.

Risk: Low

OS Vulnerable: Windows NT

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

Set 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 **Properties**.
4. Disable **Password never expires**.

A user has no password

A user has no password. This is a risk because someone can gain unauthorized access to your system if the user name is known.

Risk: Low

OS Vulnerable: Windows NT

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 **Properties**.
4. Under **Password**, enter the password.
5. Under **Verify Password**, verify the password.
6. Click **OK**.

Set 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 **Policies** menu, choose **User's Rights**.
4. Under **Minimum Password Age**, set the value to **42** days.

A user account is dormant

The user account is dormant. This means that the account has been disabled or locked out.

Risk: Low

OS Vulnerable: Windows NT

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 **Properties**.
4. Verify correct status of the **Account disabled** checkbox.
5. Verify correct status of the **Account Locked Out** checkbox.
6. Click **OK**.

User never logged on

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.

Risk: Low

OS Vulnerable: Windows NT

Fix: Remove the account.

Remove the dormant account 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**.

Group baseline was reset

This is to inform the operator that someone has reset the baseline group scan on their machine. This is a potential vulnerability. If the baseline is reset after a [trojan horse](#) is installed, the trojan horse will go undetected.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the baseline was legitimately reset. This means that you know who reset it or why it was reset.

Group added since baseline scan

A new group was added since the group baseline scan was run.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the new group was legitimately added. This means you know who added the group or why it was added.

Group deleted since baseline scan

A group was deleted since the group baseline scan was run.

Risk: Low

OS Vulnerable: Windows NT

Fix: Deleting groups may change users authority. This may also cause problems for services and DCOM applications.

Group rights changed since baseline scan

The group's rights have changed since the group baseline scan was run. This could allow users access to critical OS features.

Risk: High

OS Vulnerable: Windows NT

Fix: Check the group's rights to make sure they are correct.

Verify group right's as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Under **Groups**, select the group account.
3. From the **Policies** menu, choose **User Rights**.
4. Verify proper rights are granted to the appropriate group.

Group user changed since baseline scan

A group's membership has changed since the group baseline scan was run. This could change the access for users.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Check the group members to make sure they are correct.

Verify group members as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (Common), User Manager**.
2. Under **Groups**, select the group account.
3. From the **User** menu, choose **Properties**.
4. Verify that the group's members are correct.

Service baseline was reset

This is to inform the operator that someone has reset the baseline service scan baseline. This is a potential vulnerability. If the baseline is reset after a [trojan horse](#) is installed, the trojan horse will go undetected.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the baseline was legitimately reset. This means that you know who reset the baseline or why it was reset.

Service added since baseline scan

A service was added since the service baseline scan was run.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify that the new service was legitimately added. This means you know who added it or why it was added.

Service deleted since baseline scan

A service was deleted since the service baseline scan was run.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the deleted service was legitimately deleted. This means you know who deleted it or why it was deleted.

Service display name changed since baseline scan

The display name for the service has changed since the service baseline scan was run. A service's display name is used by user interface programs to identify the service.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the service's display name was legitimately changed. This means you know who changed it or why it was changed.

Service type changed since baseline scan

The service type has changed since the service baseline scan was run.

There are 4 service types:

- a Win32 service that runs in its own process
- a Win32 service that shares a process with other services
- a Windows NT device driver
- a Windows NT file system driver

Note that a Win32 service process can interact with the desktop.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the service's type name was legitimately changed. This means you know who changed it or why it was changed.

Service current state changed since baseline scan

A service has changed its operational state since the service baseline scan was run. A service can be in one of 7 possible states:

- **STOPPED:** The service is not running.
- **START_PENDING:** The service is starting.
- **STOP_PENDING:** The service is stopping.
- **RUNNING:** The service is running.
- **CONTINUE_PENDING:** The 'service continue' is pending.
- **PAUSE_PENDING:** The service pause is pending.
- **PAUSED:** The service is paused.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the service's current state is OK.

Verify the service's state as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (common), Windows NT Diagnostics**.
2. From the **Services** tab, click the **Services** button for application services or the **Devices** button for driver services.
3. Verify that the current state is OK.

Service control codes changed since baseline scan

The set of control codes that the service will accept and process has changed since the service baseline scan was run. Possible control codes are:

SERVICE_ACCEPT_STOP: The service can be stopped.

SERVICE_ACCEPT_PAUSE_CONTINUE: The service can be paused and continued.

SERVICE_ACCEPT_SHUTDOWN: The service is notified when system shutdown occurs.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the controls now accepted are OK.

Verify the service's state as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (common), Windows NT Diagnostics**.
2. From the **Services** tab, click the **Services** button for application services or the **Devices** button for driver services.
3. Verify that the current state is OK.

Service wait hint interval changed since baseline scan

The service wait hint interval has changed since the service baseline scan was run. The wait hint specifies an estimate of the amount of time, in milliseconds, that the service expects a pending start, stop, pause, or continue operation to take before the service makes its next call to the SetServiceStatus function with either an incremented dwCheckPoint value or a change in dwCurrentState. If the amount of time specified by dwWaitHint passes, and dwCheckPoint has not been incremented, or dwCurrentState has not changed, the service control manager or service control program can assume that an error has occurred.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the service's current state is OK.

Verify the service's state as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (common), Windows NT Diagnostics**.
2. From the **Services** tab, click the **Services** button for application services or the **Devices** button for driver services.
3. Verify that the current state is OK.

Service start type changed since baseline scan

The service start type changed since the service baseline scan was run. The start type value specifies when to start the service. One of the following values is specified:

- **SERVICE_BOOT_START**: Specifies a device driver started by the operating system loader. This value is valid only if the service type is **SERVICE_KERNEL_DRIVER** or **SERVICE_FILE_SYSTEM_DRIVER**.
- **SERVICE_SYSTEM_START**: Specifies a device driver started by the IoInitSystem function. This value is valid only if the service type is **SERVICE_KERNEL_DRIVER** or **SERVICE_FILE_SYSTEM_DRIVER**.
- **SERVICE_AUTO_START**: Specifies a device driver or Win32 service started by the service control manager automatically during system startup.
- **SERVICE_DEMAND_START**: Specifies a device driver or Win32 service started by the service control manager when a process calls the StartService function.
- **SERVICE_DISABLED**: Specifies a device driver or Win32 service that can no longer be started.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify that the Start Type is OK.

Verify the service's state as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (common), Windows NT Diagnostics**.
2. From the **Services** tab, click the **Services** button for application services or the **Devices** button for driver services.
3. Verify that the current state is OK.

Service error control changed since baseline scan

The service error control code has changed since the service baseline scan was run. The Error Control value specifies the severity of the error if this service fails to start during startup, and determines the action taken by the startup program if failure occurs. One of the following values can be specified:

- **SERVICE_ERROR_IGNORE** The startup (boot) program logs the error but continues the startup operation.
- **SERVICE_ERROR_NORMAL** The startup program logs the error and displays a message box pop-up but continues the startup operation.
- **SERVICE_ERROR_SEVERE** The startup program logs the error. If the last-known good configuration is being started, the startup operation continues. Otherwise, the system is restarted with the last-known-good configuration.
- **SERVICE_ERROR_CRITICAL** The startup program logs the error, if possible. If the last-known good configuration is being started, the startup operation fails. Otherwise, the system is restarted with the last-known good configuration.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify that the Error Control is OK.

Verify the service's state as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (common), Windows NT Diagnostics**.
2. From the **Services** tab, click the **Services** button for application services or the **Devices** button for driver services.
3. Verify that the current state is OK.

Service binary path name changed since baseline scan

The service binary path name has changed since the service baseline scan was run. The binary path name specifies the fully qualified path to the service binary file.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify that the Binary Path Name identifies the correct binary file for this service.

Verify the service's state as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (common), Windows NT Diagnostics**.
2. From the **Services** tab, click the **Services** button for application services or the **Devices** button for driver services.
3. Verify that the current state is OK.

Service load order group changed since baseline scan

A service load order group has changed since the service baseline scan was run. A service can (but need not) be a member of a load ordering group. Membership in such a group can help determine the order in which a service is loaded.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the Load Order Group is OK.

Verify the service's state as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (common), Windows NT Diagnostics**.
2. From the **Services** tab, click the **Services** button for application services or the **Devices** button for driver services.
3. Verify that the current state is OK.

Service tag ID changed since baseline scan

The service tag ID has changed since the service baseline scan was run. A Tag ID specifies a unique tag value for a service within its Load Order Group. A value of zero indicates that the service has not been assigned a tag. You can use a tag for ordering service startup within a load order group. Note that tags are only evaluated for SERVICE_KERNEL_DRIVER and SERVICE_FILE_SYSTEM_DRIVER type services that have SERVICE_BOOT_START or SERVICE_SYSTEM_START start types.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the Tag ID is OK.

Verify the service's state as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (common), Windows NT Diagnostics**.
2. From the **Services** tab, click the **Services** button for application services or the **Devices** button for driver services.
3. Verify that the current state is OK.

Service start name changed since baseline scan

The service start name has changed since the service baseline scan was run. If the service type is SERVICE_WIN32_OWN_PROCESS or SERVICE_WIN32_SHARE_PROCESS, this name is the account name in the form of "DomainName\Username", which the service process will be logged on as when it runs. If the account belongs to the built-in domain, ".\Username" can be specified. If NULL is specified, the service will be logged on as the LocalSystem account.

If the service type is SERVICE_KERNEL_DRIVER or SERVICE_FILE_SYSTEM_DRIVER, this name is the Windows NT driver object name (that is, \FileSystem\Rdr or \Driver\Xns) which the input and output (I/O) system uses to load the device driver. If NULL is specified, the driver is run with a default object name created by the I/O system based on the service name.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify that the Start Name is OK.

Verify the service's state as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (common), Windows NT Diagnostics**.
2. From the **Services** tab, click the **Services** button for application services or the **Devices** button for driver services.
3. Verify that the current state is OK.

Service owner changed since baseline scan

The owner of the service has changed since the service baseline scan was run.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify that the Owner is OK.

Verify the service's state as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (common), Windows NT Diagnostics**.
2. From the **Services** tab, click the **Services** button for application services or the **Devices** button for driver services.
3. Verify that the current state is OK.

Service DACL changed since baseline scan

The service's Discretionary Access-Control List (DACL) has changed since the service baseline scan was run.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify that the DACL is OK..

Verify the service's state as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (common), Windows NT Diagnostics**.
2. From the **Services** tab, click the **Services** button for application services or the **Devices** button for driver services.
3. Verify that the current state is OK.

Service SACL changed since baseline scan

The service's System Access-Control List (SACL) has changed since the service baseline scan was run.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify that the SACL is OK..

Verify the service's state as follows:

1. From the **Start** menu, choose **Programs, Administrative Tools (common), Windows NT Diagnostics**.
2. From the **Services** tab, click the **Services** button for application services or the **Devices** button for driver services.
3. Verify that the current state is OK.

Share baseline was reset

This is to inform the operator that someone has reset the share baseline on the machine. This is a potential vulnerability. If the baseline is reset after a [trojan horse](#) is installed, the trojan horse will go undetected.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the baseline was legitimately reset. This means that you know who reset the baseline or why it was reset.

Share added since baseline scan

A new share was added since the share baseline scan was run.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify that the new share was legitimately added. This means that you know who added the share or why it was added.

Share deleted since baseline scan

A share was deleted since the share baseline scan was run. Aside from preventing logons, deleting shares may cause problem for services or DCOM applications.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the new share was legitimately deleted. This means that you know who deleted the share or why it was deleted.

Share permissions changed since baseline scan

The share permissions have changed since the share baseline scan was run.

Risk: Low

OS Vulnerable: Windows NT

Fix: Make sure the share's permissions are correct.

Verify the share's permissions as follows:

1. In **Windows Explorer**, navigate to the share.
2. Right click the share and choose **Properties**.
3. On the **Security** tab, click the **Permissions** button.
4. Verify correct permission settings.

Share audit settings changed since baseline scan

The share audit settings have changed since the share baseline scan was run.

Risk: Low

OS Vulnerable: Windows NT

Fix: Make sure the share's audit settings are correct. This could hide security changes

Verify correct audit settings as follows:

1. In **Windows Explorer**, navigate to the share.
2. Right click the share and choose **Properties**.
3. On the **Security** tab, click the **Auditing** button.
4. Verify correct audit settings.

Share owner changed since baseline scan

The share owner has changed since the share baseline scan was run.

Risk: Low

OS Vulnerable: Windows NT

Fix: Make sure the share's owner is correct. Owners can change security settings.

Verify correct ownership as follows:

1. In **Windows Explorer**, navigate to the share.
2. Right click the share and choose **Properties**.
3. On the **Security** tab, click the **Ownership** button.
4. Verify correct ownership.

NTFS share permissions changed since baseline scan

The NTFS share permissions have changed since the share baseline scan was run.

Risk: Low

OS Vulnerable: Windows NT

Fix: Make sure the share's permissions are correct.

Verify the share's permissions as follows:

1. In **Windows Explorer**, navigate to the share.
2. Right click the share and choose **Properties**.
3. On the **Security** tab, click the **Permissions** button.
4. Verify correct permission settings.

NTFS share audit settings changed since baseline scan

The NTFS share audit settings have changed since the share baseline scan was run.

Risk: Low

OS Vulnerable: Windows NT

Fix: Make sure the share's audit settings are correct. This could hide security changes

Verify correct audit settings as follows:

1. In **Windows Explorer**, navigate to the share.
2. Right click the share and choose **Properties**.
3. On the **Security** tab, click the **Auditing** button.
4. Verify correct permission settings.

NTFS share owner changed since baseline scan

The NTFS share owner has changed since the share baseline scan was run.

Risk: Low

OS Vulnerable: Windows NT

Fix: Make sure the share's owner is correct. Owners can change security settings.

Verify correct ownership as follows:

1. In **Windows Explorer**, navigate to the share.
2. Right click the share and choose **Properties**.
3. On the **Security** tab, click the **Ownership** button.
4. Verify proper ownership.

ISS install directory not secured

The ISS install directory is not secured. The data gathered by ISS products can contain sensitive information such as passwords and machine configuration data.

Risk: Low

OS Vulnerable: Windows NT

Fix: Secure the directory to allow only the Administrators group and System have full control.

Verify the share's permissions as follows:

1. In **Windows Explorer**, navigate to the ISS install directory (**Program Files\ISS** by default).
2. Right click the share and choose **Properties**.
3. On the **Security** tab, click the **Permissions** button.
4. Provide full control to Administrators group and System only.

Startup process baseline was reset

This is to inform the operator that someone has reset the startup process baseline on their machine. This is a potential vulnerability. If the baseline is reset after a [trojan horse](#) is installed, the trojan horse will go undetected.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the baseline was legitimately reset. This means that you know who reset the baseline or why it was reset.

A new startup process was added

A new startup process was added since the process baseline scan was run. A startup process is a program that is configured to run automatically whenever Windows is started. This check detects six types of startup processes::

- Programs that are in the Common Startup Folder.
- Programs that are in the current user's Startup Folder.
- Programs that are listed in the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Registry key.
- Programs that are listed in the HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run Registry key.
- Programs that are listed in the "Load" value of the HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Registry key.
- Programs that are listed in the "Run" value of the HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Registry key.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify that the new startup process was legitimately added. This means you know who added it or why it was added.

Startup process deleted since baseline scan

A startup process was deleted since the last process baseline scan was run. Therefore, the startup process is no longer configured to run automatically whenever Windows starts.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the startup process was legitimately deleted. This means you know who deleted it or why it was deleted.

Startup process changed since baseline scan

A startup process was changed since the process baseline scan was run. If the startup process is represented by an executable file in a Startup folder (either the common startup folder or the current user's startup folder), this means that the executable file has changed. Otherwise, one of the relevant "Run" or "Load" Registry entries has been changed.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Verify that the change is acceptable. This means you know who changed it or why it was changed.

A modem was found

A modem was detected on one of the machine's COM ports.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify that the modem cannot be used to allow unauthorized remote access to the machine.

Verify remote access service settings as follows:

1. From the **Start** menu, choose **Settings, Control Panel**.
2. Open the **Network** applet.
3. From the **Services** tab, select **Remote Access Service**.
4. Click **Properties**.
5. Under **Port**, select the com port with the modem installed.
6. Click **Configure**.
7. Under **Port Usage**, click **Dial out only**.
8. Click **OK**.
9. Click **Continue**.

A modem may be on the specified COM port

A device was detected on one of the machine's COM ports but we cannot determine if it is a modem (e.g., we could not access the device because it is currently in use or is turned off).

Risk: Low

OS Vulnerable: Windows NT

Fix: If the device on the specified COM port is a modem, verify that it cannot be used to allow unauthorized remote access to the machine.

Verify remote access service settings as follows:

1. From the **Start** menu, choose **Settings, Control Panel**.
2. Open the **Network** applet.
3. From the **Services** tab, select **Remote Access Service**.
4. Click **Properties**.
5. Under **Port**, select the com port with the modem installed.
6. Click **Configure**.
7. Under **Port Usage**, click **Dial out only**.
8. Click **OK**.
9. Click **Continue**.

Found a RAS port configured to receive calls

A port on this RAS server is configured to receive phone calls.

Risk: Low

OS Vulnerable: Windows NT

Fix: If the device on the specified COM port is a modem, verify that it cannot be used to allow unauthorized remote access to the machine.

Verify remote access service settings as follows:

1. From the **Start** menu, choose **Settings, Control Panel**.
2. Open the **Network** applet.
3. From the **Services** tab, select **Remote Access Service**.
4. Click **Properties**.
5. Under **Port**, select the com port that is vulnerable.
6. Click **Configure**.
7. Under **Port Usage**, click **Dial out only**.
8. Click **OK**.
9. Click **Continue**.

Wscript Present on Web Server

Wscript.exe has been found on the web server. Script engines and command processors should not be present on a production server, and can be used to allow a user to possibly compromise the server.

Risk: Low

OS Vulnerable: Windows NT, Windows 9x

Fix: Remove **wscript.exe** from the server. Use a registry search tool to find all instances of references to **wscript.exe**, and either remove the references or change them to another association. Alternately, set the NTFS ACL to allow execution only by administrators.

Cscript present on Web Server

Cscript.exe has been found on the web server. Script engines and command processors should not be present on a production server, and can be used to allow a user to possibly compromise the server.

Risk: Medium

OS Vulnerable: Windows NT, Windows 9x

Fix: Delete the **cscript.exe** file from your system. Use a registry search tool to find all instances of references to **cscript.exe**, and either remove the references or change them to another association.

Writable Web Directory check

The metabase permissions on the web directory allow the HTTP PUT command to be executed within that directory. Any user with NTFS write permissions will be allowed to alter the files within that directory.

Risk: High

OS Vulnerable: Windows NT

Fix: Change the rights to that directory to read-only.

Change the web directory rights as follows:

1. In **Windows Explorer**, navigate to the share.
2. Right click the share and choose **Properties**.
3. On the **General** tab, under **Attributes**, click **Read-only**.
4. Click **OK**.

Executable Web Directory check

The scanner has detected an executable web directory which is not included in the Allowed Executable Paths list. Unless scripts or DLLs are present, execute permissions should not be set. Review the content, and whether the permissions are correct for this directory.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Disable the executable property for the site.

Disable the executable property as follows:

1. Open the IIS administration tool, select the site indicated by the scanner.
2. Choose Properties, and disable the executable property.
3. Verify that the site works properly.

If the directory contains static and executable content, it may be best to create a new directory for the executable content. See the Internet Information Server Resource Kit for additional details.

Basic HTTP Authentication Enabled

Basic HTTP authentication is enabled. This method of authentication can allow an attacker to sniff user credentials from network traffic. Basic authentication should only be used when other options are not available and should be used with secure HTTP.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Change to NTLM authentication in the IIS configuration.

Change from basic authentication as follows

1. From the **Start** menu, choose **Programs, Microsoft Internet Server, Internet Service Manager**.
2. Select the computer name for the WWW Service.
3. Click **Properties**.
4. On the Service tab, Under **Password Authentication**, enable **NTLM Authentication**.
5. Click **OK**.

Writable FTP Directory can be read

A writable FTP directory has been located which also has read permission. In order to prevent a FTP server from becoming a drop point for pirated software or other undesirable material, ensure that all writable directories which are accessible to anonymous users cannot be read.

Risk: Low

OS Vulnerable: Windows NT

Fix: Change the rights to that directory to read-only.

Change the web directory rights as follows:

1. In **Windows Explorer**, navigate to the share.
2. Right click the share and choose **Properties**.
3. On the **General** tab, under **Attributes**, click **Read-only**.
4. Click **OK**.

IIS Server #exec enabled

Server Side Includes (SSI) server #exec is enabled. This can pose a threat to any web server.

Risk: High

OS Vulnerable: Windows NT

Fix: Disable SSI exec or install the updated version of the FrontPage Server Extensions.

Download the updated version of FrontPage extensions as follows:

1. Open your browser.
2. Enter this address: <http://www.microsoft.com/frontpage/wpp/exts.htm>
3. Download the patch.

IIS Server Script Debugging Enabled

Server script debugging is enabled for the metabase directory indicated. This allows a client to view the source which is executed by the server. Allowing a client to debug the server source could reveal passwords and other critical information about your site.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Open the IIS administration tool. Locate the web directory which has server debugging enabled, and disable it. Note - this is often normal on a development server.

Client Script Debugging Enabled

Client script debugging is enabled for the metabase directory indicated. This allows a client to view the source which is executed by the client. This is typically not a severe problem, but could give a user more information about the web site than desired.

Risk: Low

OS Vulnerable: Windows NT

Fix: Open the IIS administration tool. Locate the web directory which has client debugging enabled, and disable it. Note - this is often normal on a development server.

Parent Paths Enabled for .asp pages

From the Windows NT 4.0 Option Pack Documentation: This identifier indicates whether ASP scripts will allow paths relative to the current directory, using the ..\ notation. Note that there is a potential security risk if this identifier is enabled, as directories and files outside of the service's root directory could become accessible. Due to an oversight, IIS installs with AspEnableParentPaths set to enabled. See Microsoft Knowledge Base article [not released yet] for further details.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Open the IIS administration tool. Locate the properties for all web sites, and disable Parent Paths for .asp pages.

Indexed Directory with .asp files

A web directory has been located which is indexed and contains .asp files. The source to .asp files can contain sensitive information about your web site, as well as user names and passwords used to access databases. If .asp files are indexed, the source can be obtained through a site search.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Open the IIS administration tool. Locate the directory reported by the scanner, and disable indexing. If content is located in that directory which should be indexed, the site may need to be reorganized. It may be helpful to create directories which contain only information which you wish indexed.

Non-anonymous FTP Login Enabled

The FTP server has non-anonymous logins enabled. An attacker can sniff user-password pairs in clear-text, or can attempt to guess passwords. Note that login attempts are processed as local logins, and it is not possible to enable account lockout on the administrator user locally. It is recommended that only anonymous FTP be enabled.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Open the IIS administration tool. Locate the FTP site with non-anonymous logins enabled, and enable only anonymous logins.

Insecure Web Password Change Enabled

This web site has password changes across an insecure connection enabled. The default is to require a SSL connection. If an intruder can sniff network traffic, user-password pairs can be gathered. By default, insecure password changes are disabled.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Open the IIS administration tool. Locate the root of the website, and require a SSL connection for all password changes.

Incoming FTP executable check

The scanner has found that a writable FTP directory allows newly created files to be executable. An attacker could use this to create executable content on your system, and then execute it through another method such as the web server.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Open Explorer. Locate the directory found by the scanner. Right-click on that directory, choose Properties, Security. Disable the execute bit for inherited file permissions.

8.3 File Names Enabled on Web Server

8.3 file name creation is enabled on this server. The NTFS file system creates DOS-style (8.3) file names which can be used by 16-bit applications to access files with names which do not fit the 8.3 convention. If the update to IIS is not applied, this can allow an intruder to access files on a server by specifying the 8.3 alias rather than the long file name. If this registry value is enabled, it will also cause a slight performance hit when files are created on the server.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Change the registry key to disable it.

Disable the registry key as follows:

1. From the **Start** menu, Click **Run**.
2. Type **regedt32** and press Enter. This opens the NT registry editor.
3. Navigate to **HKLM\System\CurrentControlSet\Control\FileSystem, NtfsDisable8dot3NameCreation**.
4. Disable the key.

Port Attack Enabled on FTP Server

From the Windows NT 4.0 Option Pack documentation: This parameter is set by default to prevent a security problem in the FTP protocol specification. The FTP service specification allows passive connections to be established based on the port address given by the client. This can allow hackers to execute destructive commands in the FTP service. The problem occurs when the FTP service connects using a port other than FTP Data port (20) and port number is less than IP_PORT_RESERVED (1024). EnablePortAttack controls if such an attack should be allowed. By default, the service does not make any connections to port numbers lower than IP_PORT_RESERVED (other than 20). If you want users to connect by using other ports as specified in the FTP RFC, this flag should be enabled.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Set the registry key.

Set the registry key as follows:

1. From the **Start** menu, Click **Run**.
2. Type **regedt32** and press Enter. This opens the NT registry editor.
3. Set the key **HKLM\System\CurrentControlSet\Services\FTPSVC\Parameters** or **HKLM\System\CurrentControlSet\Services\MSFTPSVC\Parameters, EnablePortAttack**

Microsoft Office Installed on Web Server

Microsoft Office has been found installed on the web server. If the machine being scanned is a workstation running Personal Web Server, this vulnerability may be minimal. A dedicated production web server should not have Office installed. Office exposes a large number of DCOM objects which can be used with scripting languages and may enable an attacker to subvert the web server.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Uninstall MS Office.

Developer Tools on Web Server

The scanner has found development tools on the web server. Development tools expose a number of DCOM objects which could be used by an attacker to manipulate the server. Also, if a command line is made available to a user on the server, additional executable content could be created. If this is a staging or development server, development tools are normal.

Risk: Medium

OS Vulnerable: Windows NT

Fix: If this is a production server, run the uninstall tool for the development tools. Be sure that all related registry entries are removed, or the scanner may give false positives in the future.

IIS Samples Installed on Web Server

Samples from a default IIS install were found on the web server. Sample code is not always thoroughly checked for security, and has been associated with security risks on many platforms. The phf script which came with certain distributions of Apache (see phf vulnerability) is a notable example. Although there are no currently known exploits associated with the sample code distributed with IIS 4.0, it is not good practice to leave sample code on a production web server.

Risk: Low

OS Vulnerable: Windows NT

Fix: Open the IIS administration tool and remove the IISSamples site. Also remove the physical directories associated with the site. If this is a development server, samples may be acceptable.

IUSR User in Incorrect Group

The IUSR_machine account is installed by default, and is used by Internet Information Server for unauthenticated users. This user should not be in any other groups than Guest. If IIS is installed onto a primary or backup domain controller, this user will be part of the Domain Users group, which allows this user too much access to system files and resources.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Remove the IUSR_machine user from any groups other than Guests (or Domain Guests).

Set the IUSR_machine permissions as follows:

1. [Open User Manager](#).
2. Select the IUSR_machine account.
3. Double-click on that user, and select Groups.
4. Remove the IUSR_machine user from any groups other than Guests (or Domain Guests).
5. Verify that all site functions work properly.

Browsing Enabled for Web Directory

Directory browsing was enabled for the web path reported by the scanner. Directory browsing is an inherited value which also applies to any subdirectories below this point. Any file within these directories can be viewed or downloaded.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Open the IIS administration tool. Locate the directory reported by the scanner, and disable browsing. If the directory does not have a default page, you may wish to add one.

Web Directory with no security check

The scanner has detected a Web server directory which has no access control list. This condition normally indicates that the underlying file system does not support security, and allows any user full access to all files.

Risk: Medium

OS Vulnerable: Windows NT

Fix: IIS should not be installed onto a non-NTFS file system. Convert the file system to NTFS by typing "convert [drive-letter]:" at a command line. Note - if the computer dual-boots into any other version of Windows than Windows NT, you will lose the ability to run that version of Windows. See the Internet Information Server Resource Kit for additional details.

FTP directory check

The scanner has detected a FTP server directory which has no access control list. This condition normally indicates that the underlying file system does not support security, and allows any user full access to all files.

Risk: Medium

OS Vulnerable: Windows NT

Fix: IIS should not be installed onto a non-NTFS file system. Convert the file system to NTFS by typing "convert [drive-letter]:" at a command line. Note - if the computer dual-boots into any other version of Windows than Windows NT, you will lose the ability to run that version of Windows. See the Internet Information Server Resource Kit for additional details.

Restricted Web Directory with no security

The scanner has detected a restricted Web server directory which has no access control list. This condition normally indicates that the underlying file system does not support security, and allows any user full access to all files.

Risk: Medium

OS Vulnerable: Windows NT

Fix: IIS should not be installed onto a non-NTFS file system. Convert the file system to NTFS by typing "convert [drive-letter]:" at a command line. Note - if the computer dual-boots into any other version of Windows than Windows NT, you will lose the ability to run that version of Windows. See the Internet Information Server Resource Kit for additional details.

IIS incorrect web permissions

Incorrect permissions on web directory shown.

Risk: High

OS Vulnerable: Windows NT

Fix: Secure the directory by granting access to read and execute only.

IIS incorrect permissions on restricted item

There are incorrect permissions on the displayed item.

Risk: High

OS Vulnerable: Windows NT

Fix: Secure the directory by granting access to read and execute only.

Web Directories With Crossing Paths

The scanner found two HTTP paths that point to the same physical location. If the metabase access permissions are not identical, it may be possible to obtain access through one path, but not the other. It is more difficult to maintain the web site consistently when there are multiple paths to the same physical location.

Risk: Low

OS Vulnerable: Windows NT

Fix: Verify the access permissions and controls for each path and make sure they are consistent. Either edit the URLs so that each site can point to a common resource through a single HTTP path, or adjust the permissions.

IIS Version 2 installed

IIS and PWS version 3 added many security-related fixes. Upgrade to version 3 by applying Service Pack 3, or upgrade to version 4 from NT Option Pack 4.

Risk: High

OS Vulnerable: Windows NT, Windows 95

Fix: Install IIS or PWS Version 3 or 4.

IIS CGI scripts run as system

This setting allows CGI scripts to run in the context of the system instead of HTTP user. System authority is much higher than the user authority.

Risk: High

OS Vulnerable: Windows NT, Windows 95

Fix: To correct it for IIS pre-v4, or PWS pre-v4, set the registry setting KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters key value of CreateProcessAsUser to 1.

Change the registry key as follows:

1. From the **Start** menu, Click **Run**.
2. Type **regedt32** for Windows NT or **regedit** for Windows 95 and press Enter. This opens the registry editor.
3. Navigate to KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters.
4. Double click CreateProcessAsUser
5. Set it to a value of 1.
6. Click **OK**.

IIS Special characters allowed in shell

This setting allows special characters for shell commands. This can allow users to run arbitrary commands on the system.

Risk: High

OS Vulnerable: Windows NT, Windows 95

Fix: To correct it for IIS pre-v4, or PWS pre-v4, set the registry setting HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters key value of AllowSpecialCharsInShell to 1.

Change the registry key as follows:

1. From the **Start** menu, Click **Run**.
2. Type **regedt32** for Windows NT or **regedit** for Windows 95 and press Enter. This opens the registry editor.
3. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters.
4. Double click AllowSpecialCharsInShell.
5. Set it to a value of 1.
6. Click **OK**.

pcANYWHERE32 is installed

PcANYWHERE32 is installed on the machine. This remote control software package can be used to remotely access the machine.

Risk: Low

OS Vulnerable: Windows NT, Windows 95

Fix: Verify that the software cannot be used to allow unauthorized remote access to the machine.

Carbon Copy 32 is installed

Carbon Copy 32 is installed on the machine. This remote control software package can be used to remotely access the machine.

Risk: Low

OS Vulnerable: Windows NT, Windows 95

Fix: Verify that the software cannot be used to allow unauthorized remote access to the machine.

Remotely Possible/32 is installed

Remotely Possible/32 is installed on the machine. This remote control software package can be used to remotely access the machine.

Risk: Low

OS Vulnerable: Windows NT, Windows 95

Fix: Verify that the software cannot be used to allow unauthorized remote access to the machine.

LapLink is installed

LapLink is installed on the machine. This remote control software package can be used to remotely access the machine.

Risk: Low

OS Vulnerable: Windows NT, Windows 95

Fix: Verify that the software cannot be used to allow unauthorized remote access to the machine.

Remote DeskLink for Windows 95 is installed

Remote DeskLink for Windows 95 is installed on the machine. This remote control software package can be used to remotely access the machine.

Risk: Low

OS Vulnerable: Windows 95

Fix: Verify that the software cannot be used to allow unauthorized remote access to the machine.

IIS Unauthorized ODBC Data Access with RDS and IIS

Remote Data Services implicit remote is enabled via IIS. It allows unauthorized user to access ODBC data bases via IIS. See <http://www.microsoft.com/security/bulletins/ms98-004.htm> for full details.

Risk: Low

OS Vulnerable: Windows NT, Windows 95

Fix: Delete the following registry keys: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\VbBusObj.VbBusObjCls

Delete the registry keys as follows:

1. From the **Start** menu, Click **Run**.
2. Type **regedt32** for Windows NT or **regedit** for Windows 95 and press Enter. This opens the registry editor.
3. Navigate to the key.
4. Highlight the key.
5. From the **Edit** menu, choose **Delete**.
6. Click **YES**.

Unauthorized user can debug programs.

Without this patch, unauthorized user may run published exploit tools to debug and crash programs. See security bulletin MS98-009 for details.

Risk: Low

OS Vulnerable: Windows NT

Fix: Apply the patch indicated in MS98-009.

Apply the patch as follows:

1. Open your browser.
2. Enter this URL: <http://www.microsoft.com/security/>.
3. On the left column, under **Security Bulletins**, click **security bulletins by date**.
4. Click MS98-09.
5. Under What Microsoft is Doing, select the patch appropriate for your system.
6. Follow the instructions.

Unauthorized user access IIS files

Without this patch, unauthorized user access files on the server. See security bulletin MS98-003 for details.

Risk: Low

OS Vulnerable: IIS:3.0 and earlier, Windows NT

Fix: Apply the patch indicated in MS98-003.

Apply the patch as follows:

1. Open your browser.
2. Enter this URL: <http://www.microsoft.com/security/>.
3. On the left column, under **Security Bulletins**, click **security bulletins by date**.
4. Click MS98-03.
5. Under What Microsoft is Doing, select the patch appropriate for your system.
6. Follow the instructions.

IIS Passive FTP patch not applied

This patch fixes a problem that could crash the FTP IIS service. See security bulletin MS98-006 for details.

Risk: Low

OS Vulnerable: IIS:3.0 and earlier, Windows NT

Fix: Apply the patch indicated in MS98-006.

Apply the patch as follows:

1. Open your browser.
2. Enter this URL: <http://www.microsoft.com/security/>.
3. On the left column, under **Security Bulletins**, click **security bulletins by date**.
4. Click MS98-06.
5. Under What Microsoft is Doing, select the patch appropriate for your system.
6. Follow the instructions.

IIS SSL patch not applied

This patch fixes a problem that allows decoding of SSL message. See security bulletin MS98-002 for details.

Risk: Low

OS Vulnerable: IIS:3.0 and earlier, Windows NT

Fix: Apply the patch indicated in MS98-002.

Apply the patch as follows:

1. Open your browser.
2. Enter this URL: <http://www.microsoft.com/security/>.
3. On the left column, under **Security Bulletins**, click **security bulletins by date**.
4. Click MS98-02.
5. Under What Microsoft is Doing, select the patch appropriate for your system.
6. Follow the instructions.

MIME-compliant e-mail client attachment buffer overflow

A mail or news message that contains an attachment with a very long filename could cause a MIME-compliant e-mail client to unexpectedly shut down. These very long filenames do not normally occur in mail or news messages, and must be intentionally created by someone with malicious intent. An attacker could use this malicious e-mail message to run arbitrary computer code contained in the long string.

In Security Scanner, installing the Microsoft Outlook patch fixes a problem that can crash Outlook 98 and Outlook Express 4.x when receiving files with long file names.

Risk: Low

OS Vulnerable: Windows NT, Windows 9x

Fix: Download and apply the appropriate updates listed below. Note: You should obtain these patches by downloading them from the Web sites listed below, or through some other trusted mechanism, such as through your ISP.

Microsoft Outlook: Apply the appropriate patch as indicated in Security Bulletin MS98-008 at

<http://www.microsoft.com/security/bulletins/ms98-008.asp>.

Apply the Outlook patch as follows:

1. Open your web browser.
2. Go to <http://www.microsoft.com/security/bulletins/ms98-008.asp>.
3. Under 'What Customers Should Do,' select the patch appropriate for your
4. system.
5. Follow the instructions to download and install the patch.

References: Sendmail, Inc. sendmail: Upgrade to sendmail version 8.9.1. Upgrades and patches are available from

<ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.9.1a.patch> .

A modem configured for AutoAnswer was found

A modem was detected on one of the machine's COM ports. This modem was in AutoAnswer mode.

Risk: Low

OS Vulnerable: Windows NT, Windows 9x

Fix: Verify that the modem cannot be used to allow unauthorized remote access to the machine.

Verify remote access service settings as follows:

1. From the **Start** menu, choose **Settings, Control Panel**.
2. Open the **Network** applet.
3. From the **Services** tab, select **Remote Access Service**.
4. Click **Properties**.
5. Under **Port**, select the com port that is vulnerable.
6. Click **Configure**.
7. Under **Port Usage**, click **Dial out only**.
8. Click **OK**.
9. Click **Continue**.

A modem configured for AutoAnswer was found and Dial Tone was detected on the phone line

A modem was detected on one of the machine's COM ports. This modem was in AutoAnswer mode and was connected to a phone line on which Dial Tone was detected.

Risk: Medium

OS Vulnerable: Windows NT, Windows 9x

Fix: Verify that the modem cannot be used to allow unauthorized remote access to the machine.

Verify remote access service settings as follows:

1. From the **Start** menu, choose **Settings, Control Panel**.
2. Open the **Network** applet.
3. From the **Services** tab, select **Remote Access Service**.
4. Click **Properties**.
5. Under **Port**, select the com port that is vulnerable.
6. Click **Configure**.
7. Under **Port Usage**, click **Dial out only**.
8. Click **OK**.
9. Click **Continue**.

The NTFS directory being shared is not secure

A NTFS share that has at least writable access by Guest or Everyone to the Share itself also allows Guest or Everyone at least write on the NTFS volume. If the share permission are open, the NTFS permissions should be tighter.

Risk: Low

OS Vulnerable: Windows NT

Fix: Change the NTFS permission on the directory that is shared, or change the access permission on the share.

Verify the shared directory as follows:

1. In **Windows Explorer**, navigate to share.
2. Right click the share and choose **Properties**.
3. On the **Security** tab, click the **Permissions** button.
4. Provide full control to Administrators group and System only.

AutoRun setting not default

The settings to prevent the AutoRun feature on different drive types have been changed to allow more than the default types to run. This will allow other drives to potentially run [trojan horse](#) programs.

Risk: High

OS Vulnerable: Windows NT, Windows 9x

Fix: Change the registry setting HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer, "NoDriveTypeAutoRun" to the default of 0x95.

Change the registry key as follows:

1. From the **Start** menu, Click **Run**.
2. Type **regedt32** for Windows NT or **regedit** for Windows 95 and press Enter. This opens the registry editor.
3. Navigate to **HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer**.
4. Double click **NoDriveTypeAutoRun**.
5. Set it to a default value of 0x95.
6. Click **OK**.

AutoRun is set for RAM disks

The settings to prevent the AutoRun feature on different drive types have been changed to allow RAM disks to run programs. This will allow other drives to potentially run [trojan horse](#) programs.

Risk: High

OS Vulnerable: Windows NT, Windows 9x

Fix: Change the registry setting HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer, "NoDriveTypeAutoRun". Or the value with 0x40. If using the default of 0x95, set it to 0xd5. If turned off CD-ROMs the value will be 0xb5. Change it to 0xf5.

Change the registry key as follows:

1. From the **Start** menu, Click **Run**.
2. Type **regedt32** for Windows NT or **regedit** for Windows 95 and press Enter. This opens the registry editor.
3. Navigate to **HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer**.
4. Double click **NoDriveTypeAutoRun**.
5. Set it to the appropriate value (above).
6. Click **OK**.

Other Information

Microsoft security bulletins:

<http://www.microsoft.com/security/>

Windows Update Site, <http://windowsupdate.microsoft.com>

The Java Script patch is not applied

The Java Script patch is not applied. This means your system is vulnerable to malicious intent over the Internet. Microsoft Internet Explorer 4.0, 4.01 and 4.01 SP1 use the JScript Scripting Engine version 3.1 to process scripts on a web page. When Internet Explorer encounters a web page that uses JScript script to invoke the Window.External function with a very long string, Internet Explorer or Windows 98 could terminate.

Risk: High

OS Vulnerable: Windows NT, Windows 9x

Fix: Apply the scripting patch or disable Active Scripting in the "Untrusted" and "Internet" zones.

Apply the scripting patch as follows:

1. Open your browser.
2. Enter this URL: <http://www.microsoft.com/msdownload/vbscript/scripting.asp>
3. Download the **scr31en.exe** patch (700K).
4. Once the download is complete, execute the **scr31en.exe** file.

Disable Active Scripting as follows:

1. Open Internet Explorer 4.x.
2. From the **View** menu, choose **Internet Options**.
3. Click the **Security** tab.
4. Under **Internet Zone**, click **Custom (for expert users)**.
5. Click **Settings**.
6. Under **Scripting**, navigate to **Active scripting**.
7. Click **Disable**.
8. Click **OK**.

More Information:

Microsoft security bulletins:

<http://www.microsoft.com/security/>

<http://www.microsoft.com/security/bulletins/>

Microsoft Knowledge Base (KB) article, (Q191200),

<http://support.microsoft.com/support/kb/articles/q191/2/00.asp>

Windows Update Site, <http://windowsupdate.microsoft.com>

BackOrifice Default Install Check

BackOrifice is a 'Backdoor' for Windows95 released by the hacker group 'Cult of the Dead Cow'. It allows remote users to have total control of your machine. If discovered, BackOrifice should be removed immediately.

Risk: High

OS Vulnerable: Windows 95

Fix: Remove the indicated service from the

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServiceskey.

To remove a default installation of BackOrifice from your system:

1. Open the registry editor

2. Open the key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices.
3. Look for an entry called '(Default)', with a value of '.exe'.
4. Delete this entry and reboot the machine.
5. Delete the file 'exe~1' in your windows system directory (probably c:\windows\system).

IWAM User in Incorrect Group

The IWAM_machine account is installed by default, and is used by Microsoft Transaction Server. This user should not be in any other groups than Guest and MTS Trusted Impersonators. If IIS is installed onto a primary or backup domain controller, this user will be part of the Domain Users group, which allows this user too much access to the system files and resources.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Remove the IWAM_machine user from any groups other than Guests (or Domain Guests) and MTS Trusted Impersonators.

Set the IWAM_machine permissions as follows:

[1. Open User Manager.](#)

2. Select the IWAM_machine account.
3. Double-click on that user, and select Groups.
4. Remove the IWAM_machine user from any groups other than Guests (or Domain Guests) and MTS Trusted Impersonators.
5. Verify that all site functions which rely on MTS work properly.

NetBus Installed

An installation of NetBus has been detected on the host. NetBus is a 'Backdoor' program for Windows 95 and Windows NT that, according to the NetBus web page, will let a remote user do the following things to your machine:

- Open/Close CD-ROM.
- Show optional BMP/JPG image.
- Swap mouse buttons.
- Start optional application.
- Play a wav file.
- Control mouse.
- Show different kind's of messages.
- Shut down Windows.
- Download optional file.
- Go to an optional URL.
- Send keystrokes.
- Listen for and send keystrokes.
- Take a screendump.
- Increase and decrease the sound-volume.
- Record sounds from the microphone.
- Upload optional file.
- Make click sounds every time a key is pressed.

If discovered, NetBus should be removed immediately.

Risk: High

OS Vulnerable: Windows NT and Windows 9x

Fix: Remove Netbus from your computers.

To remove NetBus from your computers:

1. [Open the registry editor](#) .
2. Go to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
3. Locate and delete a value named 'SysEdit'. This is the NetBus server signature.
4. Reboot the computer.
5. Delete the SysEdit.exe and KeyHook.dll files from your system. You can locate these files from the Start menu by choosing Find, Files or Folders. After the registry entry and server executables are deleted, NetBus is no longer installed on the system.

For more information about NetBus, the NetBus web page is at <http://netbus.hypermart.net/>

Snork denial of service attack.

The ISS X-Force has been researching a denial of service attack against the Windows NT RPC service. This attack allows an attacker with minimal resources to cause a remote NT system to consume 100% CPU Usage for an indefinite period of time. It also allows a remote attacker to utilize a very large amount of bandwidth on a remote NT network by inducing vulnerable systems to engage in a continuous bounce of packets between all combinations of systems. This attack is similar to those found in the "Smurf" and "Fraggle" exploits, and is known as the "Snork" attack. This vulnerability exists on Windows NT 4.0 Workstation and Server. All systems with service packs up to and including SP4 RC 1.99 are vulnerable, including any hotfixes released prior to 9/10/98.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Apply the Microsoft Snork patch.

Apply the patch as follows:

1. Open your web browser.
2. Navigate to <http://www.microsoft.com/security/bulletins/ms98-014.asp>.
3. Download the patch.

Windows NT 4.0 Without Service Pack 4

This host does not have Windows NT 4.0 Service Pack 4 (SP4) installed. Due to the large number of security and protocol-related fixes in Service Pack 4, it is strongly recommended that this service pack be applied. Several of these fixes are not available for Windows NT 3.51 and earlier versions, therefore it is highly recommended that any machines running versions of Windows NT prior to v4.0 be upgraded to SP4.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Apply the latest Windows NT 4.0 Service Pack.

To apply the latest Windows NT 4.0 Service Pack:

1. Open a web browser.
2. Go to <http://support.microsoft.com/support/ntserver/Content/ServicePacks/> and follow the directions to download the appropriate service pack for your computer.
3. Find the installation program you downloaded to your computer.
4. Double-click the program icon to start the installation.
5. Follow the installation directions.

More information: For general information about the vulnerabilities fixed in SP4, see Microsoft Knowledge Base Article Q150734 "List of Bugs Fixed in Windows NT 4.0 Service Pack 4 (part 1)" at <http://support.microsoft.com/support/kb/articles/Q150/7/34.asp> and Q194834 "List of Bugs Fixed in Windows NT 4.0 Service Pack 4 (part 2)" at <http://support.microsoft.com/support/kb/articles/Q194/8/34.asp> . All documents are located at <ftp://ftp.microsoft.com/bussys/winnt/winntpublic/fixes/usa/nt40/ussp4>

Windows NT 4.0 Without Service Pack 3

Windows NT was discovered without Service Pack 3 installed. Unauthorized users may gain access to the Registry. This leaves the machine vulnerable to malicious activity, including bad Server Message Block (SMB) packets or RPC Locator calls, which can cause the machine to become extremely slow.

Risk: Medium

OS Vulnerable: Windows NT

Fix: Apply the Windows NT 4.0 Service Pack 3 (SP3)

To apply Windows NT 4.0 Service Pack (SP3):

1. Open a web browser.
2. Go to <http://support.microsoft.com/support/ntserver/Content/ServicePacks/> and follow the directions to download the appropriate service pack for your computer.
3. Find the installation program you downloaded to your computer.
4. Double-click the program icon to start the installation.
5. Follow the installation directions.

More information: For more information about the vulnerabilities that are fixed in Service Pack 3, see <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ussp3/readme.txt>

NOTE: Some vulnerabilities may not apply to your configuration.

Delete Policy

At this dialog you can:

- [Remove a policy from the System Scanner database](#)

Right click on any component in this dialog for component level help.

[More on Scanning](#)

Rename Policy

At this dialog you can:

- [Choose a policy to rename](#)

Right click on any component in this dialog for component level help.

[More on Scanning](#)

Copy & Edit Policy Wizard

At this dialog you can:

- [Copy and Edit a Policy](#)

Name of new policy: Type the name of the new policy.

Policy to copy: Select the existing policy to copy.

What's This? Help

What's This? help provides help on GUI's individual components. Right click on any component in this dialog for What's This? help.

[More on Scanning](#)

Policy Wizard

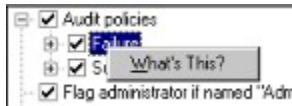
At this dialog you can configure which checks and settings to include in the policy.

How to Use the Policy Wizard

Select the check groups on the left side of the dialog and configure the checks or settings on the right side of the dialog. Some check groups do not require configuring (e.g., Denial of Service, OS Version).

What's This? Help

What's This? Help provides help on GUI's individual components. For checks, What's This? provides information such as type of check and vulnerabilities scanned when the check is enabled. For buttons and other GUI components, What's This? help provides functionality information for the component selected.



Right click on any GUI component for What's This? help (see below).

[More on Policies](#)

General Settings (Basic)

At this dialog you can:

- [Run scan at a low priority in the background](#)
- [Run a scan at system startup](#)

Policy to use: select a policy to run at system startup.

What's This? Help

What's This? help provides help on GUI's individual components. Right click on any component in this dialog for What's This? help.

General Settings (Advanced)

At this dialog you can:

- [Set the number of days for the Scan Results Database to be purged](#)
- [Manually Purge the database at any time](#)

Scan Results Database: Set the number of days for System Scanner to automatically purge the [scan results database](#).

Have scans verify that the System ScannerWin install directory is insecure: Enable this to secure the installation directory for System Scanner. When installing System Scanner on an NTFS directory, the install process sets permissions so only Administrators have full access to all the files.

Note that the install directory and registry keys are locked down. ISS recommends that you do not change the permissions.

What's This? Help

What's This? help provides help on GUI's individual components. Right click on any component in this dialog for What's This? help.

Main Window

This is the main dialog. It is displayed when System Scanner is launched. At this dialog you can:

- [Run a scan manually via the scan button bar](#)

Menu Bar

Menu Name	Description
File	Scan Now: Starts a scan. Stop Scan: Stops a scan. Pause Scan: Pauses a scan. Resume Scan: Resumes a scan. Hide Console: Minimizes GUI. Close and Exit: Closes the console and the agent.
View	Toolbar: Toolbar present when checked. Status Bar: Status bar present when checked
Policy	New: Creates a new policy. Delete: Deletes a policy. Rename: Renames a policy Edit: Edits a policy. Copy & Edit: Copies and edits an existing policy.
Settings	General: Opens general settings dialog basic and advanced. Schedule: Opens the schedule dialog.
Report	Vulnerabilities: Generates vulnerabilities report. Services: Generates services report. Trends: Generates trends report. Differential: Generates differential reports.
Help	Contents and Index: Opens the online help system. Product Updates: Begins product updates. About System Scanner for Windows: Displays version and Copyright information.

Last scan completed: Displays the time and date of the latest scan that has completed.

Policy: Displays the [policy](#) that was used during the last scan.

Termination Status: Displays the status of the last scan completed, whether it completed successfully or failed during the scan.

Vulnerabilities: This lists all of the [vulnerabilities](#) found during the scan. Vulnerabilities are listed in the order of High Severity to Low Severity.

What's This? Help

What's This? help provides help on GUI's individual components. Right click on any component in this dialog for What's This? help.

Scheduled Scan

At this dialog you can:

- [Add a scheduled scan](#)
- [Edit a scheduled scan](#)
- [Delete a scheduled scan](#)

What's This? Help

What's This? help provides help on GUI's individual components. Right click on any component in this dialog for What's This? help.

[More on Scheduling](#)

Schedule Scan

At this dialog you can:

- [Schedule a scan to run on a given \(month/day/time/frequency\)](#)

What's This? Help




What's This? help provides help on GUI's individual components. Right click on any component in this dialog for What's This? help.

[More on Scheduling](#)

Report Options

At this dialog you can select scans(s) and customize the level of detail in the reports.

Scans: A list of scans completed. Select scans from this list for reporting. Hold down the **Ctrl** key to select multiple scan results.

Component	Definition
Date	Time and date when the scan has completed
Policy	The policy used.
Comment	Optional comment describing the scan. This is entered when you run a scan.
	The scan has completed successfully.
	The scan has an error.
	The scan has been stopped. See Stopping Scans

Vulnerability Severity: You can choose high, medium, and low [risk level](#) vulnerabilities to report.

Report Detail: You can choose full description, [fix](#) information, or [policy](#) information to report.

Differential: You can choose from the following differential options::

- [Vulnerabilities in 1st Scan only](#)
- [Vulnerabilities in 2nd Scan Only](#)
- [Vulnerabilities Common to Both](#)

[More on Reporting](#)

Scan Now

At this dialog you can:

- [Scan Now](#)
- Select a policy
- Add a comment to the scan (this appears when running reports)

What's This? Help

What's This? help provides help on GUI's individual components. Right click on any component in this dialog for What's This? help.

[More on Scanning](#)

About System Scanner for Windows

This dialog displays the following

- Version of System Scanner
- Copyright Information
- Build version number

Report Export

At this dialog you can:

- [Export a report to an HTML file](#)

What's This? Help

What's This? help provides help on GUI's individual components. Right click on any component in this dialog for What's This? help.

[More on Reporting](#)

Report Disposition

At this dialog you can:

- [View a report in your web browser](#)
- [Export a report to an HTML file](#)

What's This? Help

What's This? help provides help on GUI's individual components. Right click on any component in this dialog for What's This? help.

[More on Reporting](#)

New Policy Name

At this dialog you can:

- [Enter the new name of the policy to create](#)

What's This? Help

What's This? help provides help on GUI's individual components. Right click on any component in this dialog for What's This? help.

[More on Policies](#)

New Policy Wizard

At this dialog you can:

- [Create a policy](#)

Name of new policy: type the name of the new policy.

I want the wizard to:

GUI Option

Suggest scan settings for me

Let me choose all scan settings for myself

What does it do?

The wizard automatically creates the policy based on the needs of your system.

The wizard allows you to manually create the policy.

What's This? Help

What's This? help provides help on GUI's individual components. Right click on any component in this dialog for What's This? help.

[More on Policies](#)

New Policy Wizard

At this dialog you can run the smart configuration. The smart configuration selects which [checks](#) are included in the [policy](#).

Click on the Smart Configuration button to initiate the smart configuration process.

What's This? Help

What's This? help provides help on GUI's individual components. Right click on any component in this dialog for What's This? help.

[More on Policies](#)

New Policy Wizard

I want the wizard to:

GUI Option

Save the policy without modification

Let me view/edit the policy before saving

What does it do?

The wizard save the policy without further modification

You can modify the policy manually.

What's This? Help

What's This? help provides help on GUI's individual components. Right click on any component in this dialog for What's This? help.

[More on Policies](#)

Policy Wizard

You can configure which checks and settings to include in the policy.

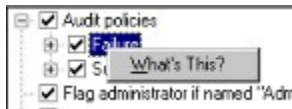
How to Use the Policy Wizard

Select the check groups on the left side of the dialog and configure the checks or settings on the right side of the dialog. Some check groups do not require configuration (e.g., Denial of Service, OS Version).

What's This? Help

What's This? help provides help on GUI's individual components. For checks, What's This? provides information such as type of check and vulnerabilities scanned when the check is enabled. For buttons and other GUI components, What's This? help provides functionality information for the component selected.

Right click on components for What's This? help (below).



[More on Policies](#)

Product Updates

At this dialog you can update the checks in System Scanner. This will accomplish 'to the minute' security for your system.

Name of product update file to run: Enter the name of the product update file.

Begin Update button: Initiates the product update. Your system's functionality will return when this process is complete.

Copy and Edit

Opens the copy & edit policy wizard. From there, you can copy and edit an existing [policy](#).

Delete

You can delete a [policy](#).

Edit

Opens the edit policy wizard. From there, you can edit a [policy](#) .

New

Opens the new policy wizard. From there, you can create a new [policy](#).

Rename

You can rename a [policy](#) .

A list of current policies in the database. From this list, select policies to rename.

{button ,AL(`configuration',0,`,`,`Main')} [More about policies](#)

Activates the next dialog which allows you to select a new name for the policy.

{button ,AL(`configuration',0,`,`')} [More about policies](#)

Enter the new name for the selected policy.

{button ,AL(` configuration',0,`,`, ` Main')} [More about policies](#)

Closes this dialog.

Applies the name change and closes this dialog.

Discards the name change and closes this dialog.

A list of current policies in the database. From this list, select policies to delete.

{button ,AL(`configuration',0,`,`Main')} [More about policies](#)

Removes the selected policy from the database.

Closes this dialog.

A list of scheduled scans. Select scans from this list to modify schedules.

{button ,JI(`sysscan.hlp`,`Scheduling_Scans`)} [More on Scheduling](#)

Adds a new scan schedule.

Modifies the selected scan schedule.

Deletes the selected scan schedule.

Closes this dialog.

Displays a description of the scheduled scan.

Select a policy to use in the scheduled scan.

Set the frequency of the scheduled scan (Daily, Monthly, or Once)

Set the time of the scheduled scan.

Set the date of the scheduled scan.

Set the day of the month for the scheduled scan.

Runs the scan on Mondays.

Runs the scan on Tuesdays.

Runs the scan on Wednesdays.

Runs the scan on Thursdays.

Runs the scan on Fridays.

Runs the scan on Saturdays.

Runs the scan on Sundays.

Saves the schedule and closes this dialog.

Discards schedule and closes this dialog.

Select the policy for scanning.

Enter a comment for this scan. The comment is used for reporting and is optional.

Starts the scan.

Cancel the scan and close this dialog.

Determines the number of days between purging the scan results database.

```
{button ,JI(`sysscan.hlp>Main`,`Scan_Result_Database_Purging`)} More on purging the Scan Results database
```


Purges the scan results database immediately.

{button ,JI(`sysscan.hlp>Main`,`Scan_Result_Database_Purging`)} [More on purging the Scan Results database](#)

Runs the scan at a low priority in the background. System Scanner places all running process as a high priority and the scan as a low priority.

Runs the scan at system startup.

Select a policy to use at the system startup scan.

Launches the report in your web browser.

Exports the report to an HTML file.

Launches the report in your web browser.

Enter the filename for the report.

Changes the directory path and filename for the report.

Includes all high risk vulnerabilities in the report.

Includes all medium risk vulnerabilities in the report.

Includes all low risk vulnerabilities in the report.

Includes a full description of vulnerabilities in the report.

Includes all fix information in the report.

Includes all policy information in the report.

A list of scans completed. Select scans from this list for reporting.

Enter the new name of the policy.

Select a policy to copy.

Select a policy to edit.

The wizard automatically creates the policy based on the needs of your system.

The wizard allows you to manually create the policy.

Enter the name of the new policy.

The wizard automatically creates the policy based on the needs of your system.

The wizard allows you to manually create the policy.




Runs the smart configuration which compiles the policy.

Displays the status of the smart configuration wizard.

Saves the policy without modification.

Allows you to modify the policy before saving.

Allows you to select exploit groups to include in the policy. Expand and collapse the tree as needed for enabling exploits. . The tri-state check box architecture is as follows:

GUI Element	Definition
	A plus sign is displayed when a tree can be expanded. Click on the plus sign to expand the tree.
	A minus sign is displayed when a tree can be collapsed. Click on the minus sign to collapse the tree.
<input checked="" type="checkbox"/> Browser	A checked box with a white background is displayed when all the sub-checks are turned on. In this example, the main browser checkbox is turned on and all browser sub-checkboxes are turned on.
<input checked="" type="checkbox"/> Browser	A checked box with a gray background is displayed when a portion of the sub-checks are turned on. In this example (see below), Internet Explorer is turned off and Netscape Navigator is turned on. 
<input type="checkbox"/> Browser	An unchecked-box without a check is displayed when all sub-checks are turned off.

{button ,JI(` sysscan.hlp>Main', `Create_a_POLICY')}& [More on policies](#)

The exploits included in each group of the exploit tree (left).

This ensures the safety of the System Scanner install directory. Any changes to this directory, after installation, will report as vulnerabilities.

This determines the level of detail displayed on the report.

This reports the vulnerabilities are common to both selected scans.

This reports the vulnerabilities that are found in the first selected scan (S1) and not in the second selected scan (S2). The formula for vulnerabilities displayed in this section is (S1 - S2).

This reports vulnerabilities that are found in the second selected scan (S2) and not in the first selected scan (S1). The formula for vulnerabilities displayed in this section is (S2 - S1).

Application Group

The application group includes the following checks:

- MS Office
- Virus Scanner
- PWS

The checks in this tree are manipulated using the [tri-state check box architecture](#).

Baseline Group

Baseline group checks are grouped as follows:

- Registry Scan
- File Scan
- Services
- Processes
- User Scan
- Group Scan
- Share Scan

The checks in this tree are manipulated using the [tri-state check box architecture](#).

Browser Group

Browser group checks are grouped as follows:

- Internet Explorer
- Netscape Navigator

The checks in this tree are manipulated using the [tri-state check box architecture](#).

Internet Protocol Group

Internet protocol group checks are grouped as follows:

- Service Scan
- FTP

The checks in this tree are manipulated using the [tri-state check box architecture](#).

Operating System Group

Operating system checks are grouped as follows:

- Denial of Service
- OS Version
- Registry Settings
- User Checks
- Share Checks
- NetBIOS

Right click on check groups in this tree for more information.

The checks in this tree are manipulated using the [tri-state check box architecture](#).

Remote Access Group

The remote access group includes the following checks:

- Modems
- pcANYWHERE32
- Carbon Copy 32
- Remotely Possible/32
- LapLink
- RAS

The checks in this tree are manipulated using the [tri-state check box architecture](#).

Starts the product update process.

Cancel the product update process.

The parameters are optional and are included in the documentation for the product update.

Close and Exit

Closes the System Scanner console and removes the tray icon from your desktop.

Close

Closes the System Scanner console on your system. The agent will remain active as a tray icon on your desktop.

Pause Scan

Pauses a scan in progress.

Resume Scan

Resumes a scan that is paused.

Show console

Displays the System Scanner console.

Start Scan

Starts a scan. You select the [policy](#) to use.

Stop Scan

Stops a scan that is running.

Product Updates

Downloads product updates to your system. These updates include the latest vulnerability checks that ensure your system's security.

Browse

You can browse the file for the product update.

Filename

The name of the program which will perform the product update. This will usually be an exe or a pfw file.

Differential

Opens the [differential_report_dialog](#) . You can create differential reports between two or more scans. See [Reporting](#)

Services

Open the [services report dialog](#) . You can view and export service report. See [Reporting](#)

Trends

Opens the trends report dialog. You can view and export trend reports between two or more scans. See [Reporting](#)

Vulnerabilities

Opens the [vulnerabilities report dialog](#) . You can view and export vulnerability reports. See [Reporting](#)

Vulnerabilities

A list of [vulnerabilities](#) found on your system during a scan. Right click or highlight a vulnerability and press F1 for more information such as [fix](#) information.

Reset Baselines

You can reset one or more [baseline scans](#) for one or more [policies](#).

Apply

Resets the baseline and allows you to choose another [policy](#) to modify.

Baselines

A list of baseline scans. Select a [baseline scan](#) to reset.

Policies

A list of [policies](#). Select a policy to modify.

OK

Saves changes to the [policies](#) and closes this dialog.

Cancel

Discards changes to policies and closes this dialog.

Schedule

You can schedule scans to run at various times and dates.

HIDD RESET BASELINES

This will reset the baselines. This is also known as locking down your system.

Copy and Edit Policy Wizard

At this dialog you can:

- [Copy and Edit a Policy](#)

Name of new policy: Type the name of the new policy.

Policy to copy: Select the existing policy to copy.

What's This? Help

What's This? help provides help on GUI's individual components. Right click on any component in this dialog for What's This? help.

{button ,AL(`configuration',0,`,`, `Main') } [More on Scanning](#)

Passwords

The password group includes password checks for Microsoft Windows NT and Windows 9x operating systems.

What's This? Help

What's This? help provides a list of vulnerabilities detected when a check is included in a scan policy. Right click on checks in this dialog for What's This? help.

Backdoor

This check group detects backdoor programs such as:

- Back Orifice.
- NetBus

The checks in this tree are configured using the [tri-state check box architecture](#).

Copyright Information

[System Scanner for Windows](#) is a trademark of Internet Security Systems, Inc. Microsoft Access, Windows and Windows NT are trademarks of Microsoft Corporation. Java and JavaScript are trademarks of Sun Microsystems, Inc. in the United States and other countries.

All other names mentioned in this document are brands, products, and trademarks or registered trademarks of their respective holders and should be noted as such.

Copyright © 1996-1999 Internet Security Systems, Inc. All Rights Reserved.

Designed for



Microsoft®
BackOffice®

System Scanner is Microsoft BackOffice certified.

Disclaimer

ISS recommends reading the disclaimer.

{button ,JI(`s3win.HLP>Main`,`Disclaimer`)} [Disclaimer](#)

Questions?

Contact us at:

ISS Technical Support: 1(888)447-4861

Hours: 9:00 to 6:00 P.M. ET.

E-mail: support@iss.net

Sales Contact Information

Contact us at:

Hours: 9:00 to 6:00 P.M. E.T.

E-mail: sales@iss.net

{button ,KL(`legal issues in running System Scanner`,0`,`Main`)} [Legal issues in running System Scanner](#)

{button ,AL(`getting started`,0`,`Main`)} [Getting Started](#)

Disclaimer

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Internet Security Systems, Inc. The views and opinions of authors expressed herein do not necessarily state or reflect those of Internet Security Systems, Inc., and shall not be used for advertising or product endorsement purposes.

Links to Internet resources are inspected thoroughly prior to Internet Scanner's release, but the ever-changing nature of the Internet prevents Internet Security Systems from guaranteeing the content or existence of the resource. When possible, the reference contains alternate sites or keywords that could be used to acquire the information by other methods. If you find a broken or inappropriate link, please e-mail the topic name, link, and its behavior to support@iss.net.

{button ,AL(`getting started',0,`,`Main')}} [Getting Started](#)

About System Scanner

System Scanner for Windows runs on the Microsoft's Windows 95, Windows 98, and Windows NT operating systems. It is a security assessment solution from Internet Security Systems, Inc. (ISS). System Scanner evaluates the security profile of your system from the operating system (OS) perspective.

Assessments

System Scanner assesses file permissions, file ownership, network service configurations, account setup, security patches, vulnerable programs, and common user-related security weaknesses such as guessable passwords. System Scanner also looks for signs that a hacker may have broken into a system by running [baseline scans](#).

{button ,AL(` getting started',0,`,`, `Main')}} [Legal Issues in Running System Scanner](#)

{button ,AL(` getting started',0,`,`, `Main')}} [Getting Started](#)

Year 2000 Compliance

Internet Security Systems, Inc. is committed to producing the highest quality software products and services. We have recognized the issues and potential problems associated with the storage and calculations of dates with two digit year fields (Year 2000 problem). All dates used within ISS products use a standard four digit year or system specific representation that does not use the mmddyy or ddmmyy format.

Each ISS product (Internet Scanner, RealSecure, System Scanner) has been tested by configuring a test environment with the system dates on the test computers set to various dates in the 21st century. The products were then put through a regression test and the output verified with previous test runs with no errors. There are no input fields in the ISS products that require date input so no input data testing was required.

ISS has tested and verified that its SAFESuite products are "Year 2000" compliant and will not incur errors or incorrect calculations caused by wrapping the century date, failure to recognize 2000 as a leap year, or errors in computing dates.

{button ,AL(`getting started',0,`,`Main')}} [Getting started](#)

Managing Your Risks

Managing security risk in dynamic network environment requires a continual process that identifies security weaknesses, advises on severity levels, and directs the operator to the appropriate solution. The process must also identify active threats and respond before online assets are at risk – as well as confront the latest security issues with concrete, accurate, information.

This process is called [Adaptive Security Management](#) .

Adaptive Security Management

The Adaptive Security Model provides real-time monitoring, detection, and response to vulnerabilities and intrusions. The company that first made it possible was ISS, answering a widespread need for a new approach to maintaining a secure open-system data environment.

Throughout the industry, a dramatic shortage of security expertise had become drastically apparent. Coupled with the prevalence of constantly growing networks – and the ever-quickenning evolution of security threats – it had become clear the industry was ready for a breakthrough. It came from ISS.

Adaptive Security Management is an ideology composed of four integrated ISS approaches. End-to-end network security requires the ongoing and comprehensive detection of security risks. For this to be possible, frequent, automated network scanning technology is implemented first. Second, responses to security weaknesses are provided for immediate correction. Next, real-time intrusion detection occurs around-the-clock, for both internal and external attacks. And finally, self-correction in response to security threats, including active connection termination, is automatic and dynamic.

Contrary to popular network security myths, there is no single “silver bullet” able to bring about zero risk to your network. Due to the dynamic nature of networks and technologies, this ideal, while certainly attractive, is indeed impossible. Risk is proportional to vulnerabilities and threats.

For more information about Adaptive Security Management and its overall value-added and associated risk mitigation, contact ISS at sales@iss.net or <http://www.iss.net>.

{button ,AL(` security',0,`,`Main')} [More on security](#)

{button ,AL(` getting started',0,`,`Main')} [Getting started](#)

Security Cycle

Monitor

A monitoring solution is used to watch for new security breaches or attempts to abuse old vulnerabilities. This discipline keeps the Security Administrator in touch with the state of the network.

Detect

Software is used to detect the holes in a network. Security detection establishes a baseline security measurement.

Respond

An essential step of Continuous Security Improvement (CSI) is to monitor and respond to unauthorized access. Measurable feedback is another essential component of the CSI process. Once you have established a security policy and deployed enforcement tools, it is vital that you evaluate how well they are performing. Is the security enforcement meeting policy expectations? How should the security policy change over time? What new threats and vulnerabilities need to be considered?

{button ,AL(` security',0,`,`Main')} [More on security](#)

{button ,AL(` getting started',0,`,`Main')} [Getting started](#)

The Need for Periodically Scanning

The need for periodic scanning is based on your system's level of exposure to the Internet, the value of information on your system, and the frequency of changing software on your system. If your computer is highly exposed to the Internet, contains valuable information, or contains very [dynamic software](#) then you should scan periodically.

Scheduling Scans

You can schedule scans to run at system start-up, manually, at a low priority in the background, or scheduled to run on a time/day of the year.

{button ,AL(` scanning',0,`,` ,` Main') } [More on scanning](#)

Legal Issues in Running System Scanner

In most cases, the United States Government has upheld the right of individuals to monitor their own networks. The general consensus is all users should be notified of monitoring activities. Consult a lawyer if there are any questions as to the legality of using System Scanner for Windows on your network. For an explanation of the legal issues in running System Scanner, refer to CERT advisory CA 92:19, 'Keystroke Logging Banner', available at:

<http://www.cert.org/advisories/CA-92.19.Keystroke.Logging.Banner.Notice.html>

or

ftp://ftp.cert.org/pub/cert_adviseries/CA-92%3A19.Keystroke.Logging.Banner.Notice

{button ,AL(`getting started',0,`,`Main')}} [Getting started](#)

Vulnerability Checks

System Scanner scans for security holes that place your system at risk of future compromise by checking for vulnerabilities. System Scanner includes the following groups of checks:

- [Internet Protocol Checks](#)
- [Browser Checks](#)
- [Operating System Checks](#)
- [Application Checks](#)
- [Baseline Checks](#)
- [Remote Access Checks](#)

{button ,AL(`getting started',0,`,`Main')} [Getting started](#)

Obtaining Patch Information

In the Vulnerabilities section of the Help, you can look up specific vulnerabilities and get instructions for how to fix them. Web links are provided, where possible, to make it easy for you to go directly from the Help to the correct patch or Web Page for your problem.

Different Patch Versions

Since System Scanner can be used in many different countries, it is not always possible to go directly to a non-US patch site. If you need non-US patches, they are generally available by navigating up a few directories from the link we provide (in the case of ftp sites), or accessing the vendor's home page and navigating to the appropriate directory for your home country.

If you are not sure which version of a patch to use on your system, please contact your vendor for assistance.

Microsoft Patches

Domestic and international service packs for Windows systems are available from <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/>.

CERT Advisories

The CERT Coordination Center compiles advisories about subjects related to computer security. Its home page is <http://www.cert.org>, and advisories are stored at ftp://ftp.cert.org/pub/cert_advisories/

NT Security FAQ

This list provides answers to many questions about Windows NT security. It also includes numerous links to related security sites. It's at <http://www.it.kth.se/~rom/ntsec.html>

General Security FAQs

<http://www.iss.net/vd/faq.html>

<http://www.alw.nih.gov/Security/>

Books

Windows NT Security

Edwards, Mark Joseph: Internet Security with Windows NT Published by Duke Press, ©1997 ISBN 1-882419-62-6

Rutstein, Charles B: Windows NT Security : A Practical Guide to Securing Windows NT Servers and Workstations Published by Computing McGraw-Hill, ©1997 ISBN: 0070578338

Honeycutt, Jerry; Farrell, Bernard; Kennelly, Rich; and Millsaps, Jerry: Windows 95 and NT 4.0 Registry & Customization Handbook Published by Que Corp, ©1997 ISBN: 0789708426

Sutton, Stephen A.: Windows NT Security Guide Published by Addison-Wesley Pub Co, ©1996 ISBN: 0201419696

Sheldon, Thomas: Windows NT Security Handbook Published by Osborne McGraw-Hill, ©1996 ISBN: 0078822408

Miscellaneous

Garfinkel, Simson and Spafford, Gene: Practical UNIX & Internet Security Published by O'Reilly & Associates, Inc., ©1996 ISBN: 1565921488

Chapman, D. Brent and Zwicky, Elizabeth D.: Building Internet Firewalls Published by O'Reilly & Associates. Inc., ©1995 ISBN: 1565921240

System Requirements

You must satisfy the system requirements before you can successfully install and run System Scanner on your machine. The system requirements below present all required and recommended features needed for System Scanner. Meeting the recommended requirements increases the performance and reliability of System Scanner.

{button ,JI(` >Second', `Windows_9x_Requirements')} [Windows 9x Requirements](#)
{button ,JI(` >Second', `Windows_NT_Requirements')} [Windows NT Requirements](#)
{button ,JI(` >Second', `NT_Server_Requirements')} [NT Server Requirements](#)
{button ,JI(` >Second', `Windows_2000_Requirements')} [Windows 2000 Requirements](#)

If your system meets or exceeds these recommendations and is not operating as expected, contact technical support tsupport@iss.net .

{button ,AL(` getting started',0,`,`Main')} [Getting started](#)

Windows 9x Requirements

Required

- 486/25MHz or better processor
- 8 MB of RAM
- 25 MB of disk space for database entries
- TCP/IP installed

Recommended

- Pentium class processor
- 16 MB of RAM
- 35 MB of disk space for database entries
- TCP/IP installed

{button ,AL(` getting started',0,`,`Main')}} [Getting started](#)

Windows NT Requirements

Required

- Pentium class processor
- 8 MB of RAM
- 25 MB of disk space for database entries
- TCP/IP installed

Recommended

- Pentium class processor
- 32 MB of RAM
- 35 MB of disk space for database entries
- TCP/IP installed

{button ,AL(` getting started',0,`,`Main')}} [Getting started](#)

NT Server Requirements

Required

- Pentium class processor
- 16 MB of RAM
- 25 MB of disk space for database entries
- TCP/IP installed

Recommended

- Pentium class processor
- 32 MB of RAM
- 35 MB of disk space for database entries
- TCP/IP installed

{button ,AL(` getting started',0,`,`Main')}} [Getting started](#)

Windows 2000 Requirements

Required

- Pentium class processor
- 32 MB of RAM
- 25 MB of disk space for database entries
- TCP/IP installed

Recommended

- Pentium class processor
- 64 MB of RAM
- 35 MB of disk space for database entries
- TCP/IP installed

{button ,AL(` getting started',0,`,`Main')}} [Getting started](#)

Using Your License Key

What is a Key File?

A key file defines your licensing for System Scanner. It contains information such as the IP address of your system, which features are available, customer information, and expiration date.

You cannot use System Scanner without a key. For evaluation mode, you must obtain an evaluation key. Running System Scanner in evaluation mode lets you create and modify policies only, and does not enable scanning.

Obtaining a Key File

To use System Scanner to its full capacity, you must register the program by obtaining a new key or by updating an existing key. However, if you are only interested in testing the product, or you are not yet familiar with how the product works, you can continue to use System Scanner as evaluation software.

{button ,JI(`s3win.HLP>Third',`Obtaining_and_Installing_a_New_Key')}} [Obtaining and Installing a New Key](#)

{button ,AL(`keys',0,`,`Main')}} [More on keys](#)

Product-Updates

Product updates ensure System Scanner is checking your system for the latest [vulnerabilities](#) . By installing product updates, you are provided with the most recently discovered vulnerability checks and [fix](#) information To provide maximum security against evolving hacker techniques, install micro updates which are available from Internet Security Systems, Inc. (<http://www.iss.net>).

{button ,JI(` sysscan.HLP>Third', `download_exploit_dlls')} [Procedure](#)

{button ,AL(` configuration;scanning',0,`,`Main')} [Related topics](#)

To Install Product-Updates:

1. From the **Help** menu, choose **Product Updates**.
2. Under **Name of product update file to run**, type the name of the product update or click browse to find it.
3. Under **Parameters for product update file (optional)**, enter parameters define in the product update documentation.
4. Click **Begin Update**.
5. Click **Close**.

Obtaining and Installing a New Key

If you are a new customer, then you must request from ISS a key that licenses your software. To obtain and install your key, you must:

1. [Register your customer license.](#)
2. [Choose a method to receive your key.](#)
3. [Request a new key from the ISS License Registration web site.](#)
4. [Install the key on your system.](#)

Securing the Installation Directory

You can have scans verify that the System Scanner installation directory is secure: When installing System Scanner on an NTFS directory, the install process sets permissions so only Administrators have full access to all the files.

Note that the install directory and registry keys are locked down. ISS recommends that you do not change the permissions.

{button ,JI(`sysscan.hlp>third`,`Securing_the_Installation_Directory')} [Procedure](#)

Register Your Customer License

Before you register your customer license, make sure you have the following information handy:

- Customer contact information
- Maintenance billing contact information (optional)
- Network IP Address Range(s)

{button ,JI(`sysscan.hlp>Third', `Registering_Your_License_Procedure')}] [Procedure](#)

{button ,AL(`keys',0,`,`, `Main')}] [More on keys](#)

Choose a Method to Receive Your Key

You should use the most secure method available to download your key. Choose one of the following methods to receive your key. These methods are listed from most secure to least secure:

- Download your key with your browser. This is the preferred method since it takes advantage of the built-in Secure Sockets Layer (SSL) security in your browser.
- Have your key sent by ISS via e-mail with PGP encryption. If you have previously provided us keys@iss.net with your public PGP key, ISS Key Files sent to your e-mail address will then be sent PGP encrypted.
- Have your key sent by ISS via e-mail without encryption. We offer this option as a convenience although we acknowledge that keys sent without encryption may potentially be intercepted and compromised.
- Copy and paste the key from text displayed in your browser.
Caution: Using this method may not ensure the integrity of your key file.

{button ,JI(`sysscan.HLP>main', `Requesting_a_Key_from_the_ISS_Website')} [Requesting a key from ISS Web Site](#)

{button ,AL(`keys',0,`,`Main')} [More on keys](#)

Request a Key from the ISS Web Site

Once you have decided which method you want to use to download your key, request a new key from the ISS Registration Center at <https://www1.iss.net/lrc/>.

Prerequisite

You must know your Order Confirmation Number (OCN), your OCN Password, and the secured URL for ISS's License Registration Center (LRC). This information is written on the packing list that was sent in the package containing your software and user guide.

Missing OCN or LRC information?

If you are missing the Order Confirmation Number or the License Registration Center URL, please contact ISS at keys@iss.net . ISS will send them to you by way of e-mail, phone, fax, or overnight shipment.

{button ,AL(` keys',0,`,` Main')}} [More on keys](#)

Registering Your License

1. Print the ISS License Registration Form at <https://www1.iss.net/help/regform.html>
2. Fill out the form.
3. Fax it to the number listed on the form.

ISS will contact you by telephone to give you your OCN and password.

Install Your Key

After you have received your new or updated key file, you must install the key to make your software run at full capacity.

[Procedure](#)

[More on Keys](#)

Installing Your Key

1. Open the file in a text editor, such as Notepad.
2. Make sure that the file has a "BEGIN" line and an "END" line.
3. Save the file as "iss.key" (include the quotation marks) in the directory that contains your ISS software (by default, C:\Program Files\ISS\System Scanner). The double quotes are necessary to prevent your text editor from using an incorrect file name extension.

ISS's Recommended Security Assessment Approach

To ensure that System Scanner is used at its full potential, ISS has developed a recommended security assessment approach.

ISS recommends the following approach:

1. Run a scan on your system using the [User - Desktop Workstation](#) policy. This will determine all desktop related vulnerabilities.
{button ,JI(`>Third', `Installing_Your_Key_Procedure')} [Procedure](#)
2. Correct the vulnerabilities found during the scan.
Refer to Correcting Vulnerabilities
3. Reset the baselines. This will avoid false positives during the next scan.
{button ,JI(`s3win.HLP>Third', `Shortcut_for_Resetting_the_Baseline')} [Procedure](#)
4. Run the scan the second time to verify that all the vulnerabilities have been corrected.
{button ,JI(`s3win.HLP>Third', `Manually')} [Procedure](#)
5. Repeat steps two through four until your system is secure (free of [vulnerabilities](#)) or until you are satisfied with the risk level and number of vulnerabilities that remain.
6. Generate a Vulnerability report to view the security status of your system.
{button ,JI(`s3win.HLP>Third', `Vulnerability_Reports_View_Procedure')} [Procedure](#)
7. Create your own scan policies to further customize System Security Scanner based on your security needs.
{button ,JI(`s3win.HLP>Third', `Delete_a_POLICY_Procedure')} [Procedure](#)
8. Once you are satisfied with the scan policy that best suites your security needs, schedule it to run on a daily basis. This will ensure that your system remains at a controlled level of security.
{button ,JI(`s3win.HLP>Third', `Add_a_Scan_Schedule_Procedure')} [Procedure](#)

{button ,AL(`configuration;scanning',0,`,`Main')} [Related topics](#)

Working with Policies

[Policies](#) are needed for scanning. You specify the policy, in the GUI, when scheduling or running scans. System Scanner includes the following default policies

System Scanner supports:

{button ,JI(`sysscan.HLP>main',`Create_a_POLICY')} [Creating policies](#)

{button ,JI(`sysscan.HLP>main',`Edit_a_POLICY')} [Editing policies](#)

{button ,JI(`sysscan.HLP>main',`Copying_and_Editing_POLICYS')} [Copying and editing policies](#)

{button ,JI(`sysscan.HLP>main',`Deleting_POLICYS')} [Deleting policies](#)

{button ,JI(`sysscan.HLP>main',`Renaming_POLICYS')} [Renaming policies](#)

{button ,AL(`getting started',0,`,`Main')} [Getting started](#)

{button ,AL(`policies',0,`,`Main')} [More on default policies](#)

Generating the Baseline Database

The [baseline database](#) is generated when you run [baseline scans](#). The types of baselines are:

- [share scan baselines](#)
- [user scan baselines](#)
- [group scan baselines](#)
- [services baselines](#)
- [file scan baselines](#)
- [registry scan baselines](#)
- [process baselines](#)

When running a baseline scan, System Scanner compares the current system environment with the “snapshot” stored in the database (from the last baseline scan). [Vulnerabilities](#) are reported for every inconsistency found between the baseline database and your current system environment.

WARNING: If you fail to reset the baseline after changing your system environment, all changes will report as vulnerabilities during the next [baseline scan](#) .

{button ,AL(`baseline',0,`,`Main')} [Resetting the baselines](#)

Creating Policies

Create [policies](#) so you can run [custom scans](#) on your system. A policy must be present in order for System Scanner to scan the machine.

Automatically Creating Policies

System Scanner automatically configures policies in a method most effective for your system. It does this by performing a smart configuration process to see what is installed on your system and decides which [checks](#) to include in the policy.

{button ,JI(`sysscan.HLP>Third', `Smart_Configuration_New')} [Procedure](#)

Manually Creating Policies

You can manually configure the [checks](#) in the policy to any level of detail.

{button ,JI(`sysscan.hlp>Third', `Detailed_Configuration_New')} [Procedure](#)

{button ,AL(`configuration',0,`,`Main')} [Related topics](#)

Editing Policies

You can edit [policies](#) when you want modify the [checks](#) based on the need of your system. You can edit policies using the two methods explained below.

Automatically Editing Policies

System Scanner automatically configures policies in a method most effective for your system. System Scanner performs a smart configuration process to see what is installed on your system and decides which [checks](#) to include in the policy.

{button ,JI(`sysscan.hlp>Third', `Detailed_Configuration_New')} [Procedure](#)

Manually Editing Policies

You can manually modify the [checks](#) in the policy to any level of detail.

{button ,JI(`sysscan.hlp>Third', `Detailed_Configuration_New')} [Procedure](#)

{button ,AL(`configuration',0,`, `Main')} [Related topics](#)

Copying and Editing Policies

You can copy an existing [policy](#) to a different name and then customize it from there. This is useful when you need to create a new policy with similar [check](#) settings as an existing policy.

{button ,JI(`sysscain.HLP>Third', `Smart_Configuration_CpyEdt')}} [Procedure](#)

{button ,AL(`configuration',0,`,`, `Main')}} [Related topics](#)

Deleting Policies

You can deleting a [Policy](#) to remove it from the list of policies. Once a you delete a policy, it is not retrievable. `{button ,JI(`sysscan.HLP>Third`,`Delete_a_POLICY_Procedure')}` [Procedure](#)

WARNING: Deleting all policies disables scanning capability. Scanning is restored when a policy is created.

`{button ,AL(`configuration',0`,`Main')}` [Related topics](#)

Renaming Policies

You can rename a [Policy](#) to change the name and update the policy lists.

{button ,JI(`sysscan>Third.HLP`,`Rename_a_POLICY_Procedure`)} [Procedure](#)

{button ,AL(`configuration',0`,`Main'`)} [Related topics](#)

Scheduling Scans

When scheduling scans, System Scanner performs the scan automatically based on the schedule you define. Scheduling scans is useful when your system is subject to very little or no supervision.

Scheduling options include:

- description
- policy
- frequency (daily, weekly, monthly)
- time, and
- day (Sunday through Monday)

WARNING: You must have the System Scanner Agent installed before you can schedule scans. Without the System Scanner Agent, scheduled scans will be ignored.

Adding Schedules

You can add a schedule to the list of scheduled scans.

{button ,JI(`sysscan.HLP>Third',`Add_a_Scan_Schedule_Procedure')} [Procedure](#)

Modifying Schedules

You can modify an existing schedule from the list of scheduled scans.

{button ,JI(`sysscan.HLP>Third',`Modify_a_Schedule')} [Procedure](#)

Deleting Schedules

You can remove a schedule from the list of scheduled scans. Once a schedule is removed, it is not retrievable.

{button ,JI(`sysscan.HLP>Third',`Delete_a_Schedule_Procedure')} [Procedure](#)

{button ,AL(`configuration',0,`,`Main')} [Related topics](#)

Running Scans

Running scans on your system identifies security risks ([vulnerabilities](#)) that allow an intruder to gain unauthorized access. Scans should be run as frequently as needed (see [The Need for Periodic Scanning](#)). You can run scans using one of the methods explained below.

Running Scans at System Startup

You can run scans at system start-up to insure new vulnerabilities are detected every time your system is started. This is most effective on a system that is frequently powered ON and OFF.

```
{button ,JI(`sysscan.HLP>Third`,`At_System_Startup')}} Procedure
```

Running Scans Manually

You can run scans manually, at any time, to detect vulnerabilities on your system every time the scan is run.

```
{button ,JI(`sysscan.HLP>Third`,`Manually')}} Procedure
```

Running Scans at a Low Priority in the Background

You can run scans at a low priority in the background when your system's resources (processing power and memory) are limited. This way, scans run automatically while your system is not busy or has been idle for a period of time.

```
{button ,JI(`sysscan.HLP>Third`,`At_a_Low_Priority_in_Background')}} Procedure
```

```
{button ,AL(`scanning',0,`,`Main')}} More on scanning
```

Correcting Vulnerabilities

When to correct vulnerabilities

You should correct [vulnerabilities](#) after you perform a scan. System Scanner provides fixes needed to correct each vulnerability it detects. Refer to [Running Scans](#).

Types of corrective actions

The [fixes](#), provided by System Scanner, require you to perform the following types of corrective actions:

- [Editing the registry](#)
- [Applying patches](#)
- [Setting file permissions](#)
- [Running the User Manager \(Windows NT\)](#)
- [Running the Policy Editor \(Windows 95 & 98\)](#)

Editing the Registry

Why edit the registry?

Edit the [registry](#) to correct registry-related vulnerabilities that System Scanner detects on your system. Registry-related vulnerabilities are fabricated by your registry settings, which means you must perform registry changes to correct them.

Opening the registry

{button ,JI(`s3win.HLP>Third`,`To_open_the_registry_editor_')} [Procedure](#)

{button ,AL(`correcting',0`,``,`Main')} [More on Correcting Vulnerabilities](#)

Applying Patches

Why apply patches?

You should apply [patches](#) to correct patch-related vulnerabilities that System Scanner detects on your system.

Example

An example of a patch is Windows NT Service Pack 3 (SP3). SP3 is provided by Microsoft and available for download.

Non-example

A non-example of a patch is a request for a newer version of software (e.g., upgrade your software from v1.0 to v3.0).

Applying Patches

You should apply patches to correct patch-related vulnerabilities that System Scanner detects on your system.

{button ,JI(`s3win.HLP>Third`,`Applying_Patches_Procedure')}} [Procedure](#)

{button ,AL(`patches',0`,`>Main')}} [More on Patches](#)

{button ,AL(`correcting',0`,`Main')}} [More on Correcting Vulnerabilities](#)

To apply patches:

1. Open your Web browser.
2. Go to the Uniform Resource Locator (URL) address specified in the fix procedure. The URLs are both Hyper Text Transfer Protocol (HTTP) and File Transfer Protocol (FTP) addresses.
3. Follow the Web site instructions for downloading the patch. The name of the patch is specified in the fix procedure.
4. When downloading the patch and save it to a temporary directory (e.g., c:\temp\) on your hard drive.
5. Exit the Web browser.
6. Navigate to the location where you downloaded the patch.
7. Double click on the executable file and follow directions.
8. Repeat steps one through eight for each patch-related vulnerability.

Internet Sites

Security Mailing Lists

ISS maintains a number of Internet mailing lists on security-related topics. To discover what lists are available, or to sign up for one or more lists, see <http://www.iss.net/vd/maillist.html>.

ISS Security Library

ISS provides a wealth of site links, articles, presentations, and more at <http://www.iss.net/vd/library.html>.

Manufacturer Patches

Many manufacturers provide a central repository for their software updates. Here are a few of the manufacturers mentioned in System Scanner:

Manufacturer	URL
Microsoft Service Packs	http://support.microsoft.com/support/ntserver/Content/ServicePacks/Where.asp
Microsoft Post SP2 patches	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP2
Microsoft Post SP3 patches	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3
Microsoft Internet Explorer patches	http://www.microsoft.com/msdownload/iesecurity/iepptsecurity.htm
Microsoft 95 Patches	http://www.microsoft.com/windows95/info
Latest Microsoft Security Patches	http://micorsoft.com/security , under View by date.

{button ,AL(` patches',0,`, `Main') } [More on Patches](#)

Setting File Permissions

Why set file system properties?

System Scanner requires you to set file system properties to correct file system-related [vulnerabilities](#) . Specific changes are explained in the vulnerability [fix](#) information.

Opening File System Properties

You should open the file system properties to correct file system-related vulnerabilities that System Scanner detects on your system.

{button ,JI(`s3win.HLP>Third`,`Opening_File_System_Properties')}} [Procedure](#)

{button ,AL(`correcting',0,`,` Main')}} [More on Correcting Vulnerabilities](#)

Running the User Manager (Windows NT)

Why run the User Manager?

System Scanner requires you to run [User Manager](#) to correct related [vulnerabilities](#). The corrections needed are explained in the vulnerability fix information provided in the online help and reports.

Opening the User Manager

You should open the User Manager to correct related vulnerabilities System Scanner detects on your system.

{button ,JI(`s3win.HLP>Third`,`To_start_the_User_Manager_program')}} [Procedure](#)

{button ,AL(`correcting',0`,`Main')}} [More on Correcting Vulnerabilities](#)

Running the Policy Editor (Windows 95 and Windows 98)

Why run the Policy Editor?

Run the Policy Editor to correct related [vulnerabilities](#) that System Scanner detects on your system.

Policy Editor functions

The Policy Editor supports many functions. A portion of these functions include:

- Access Control
- Logon settings
- Password settings
- Hardware and Software settings
- User settings

Opening the Policy Editor

You should open the Policy Editor to correct the Policy Editor-related vulnerabilities.

{button ,JI(`s3win.HLP>Third`,`Opening_the_Policy_Editor`)} [Procedure](#)

{button ,AL(`correcting`,0`,`Main`)} [More on Correcting Vulnerabilities](#)

Viewing the Status of the Scan

The [Main window](#) displays the status of a scan in progress by means of the progress bar. The results of the last completed scan and the policy used are displayed above the progress bar.

{button ,AL(`reporting',0,`Main,')} [More on reporting](#)

Generating Reports

Reports provide you with all the information needed to perform security assessment on your system. Once you run a scan, results are stored into the [scan results database](#) for a period of time. You can generate reports from the scan results database and [view reports](#) or [export reports](#).

Types of Reports

With System Scanner, you can generate four types of reports:

- [Vulnerabilities Report](#)
- [Services Report](#)
- [Trends Report](#)
- [Differential Report](#)

{button ,AL(`reporting',0,`Main,')} [More on reporting](#)

Viewing Reports

Reports are viewed as standard [HTML](#) in your web browser. Below are links to procedures on how to view vulnerability reports, service reports, trend reports, and differential reports.

Viewing Vulnerability Reports

Vulnerability reports show you all vulnerabilities found on your system along with step by step [fix information](#).

{button ,JI(`sysscan.HLP>Third`,`Vulnerability_Reports_View_Procedure')}} [Procedure](#)

Viewing Service Reports

Service reports show you all services running on your system that are vulnerable.

{button ,JI(`sysscan.HLP>Third`,`Services_Report_View_Procedure')}} [Procedure](#)

Viewing Trend Reports

Trend reports show you the history change between selected scan results.

{button ,JI(`sysscan.HLP>Third`,`Trend_Reports_View_Procedure')}} [Procedure](#)

Viewing Differential Reports

Differential reports show you the differences between two scan results.

{button ,JI(`sysscan.HLP>Third`,`Differential_Reports_View_Procedure')}} [Procedure](#)

{button ,AL(`reporting',0,`Main,'')} [More on reporting](#)

Exporting Reports

Reports are exported to a standard HTML file and are viewed in your web browser. Below are links to procedures on how to export vulnerability reports, service reports, trend reports and differential reports.

Exporting Vulnerability Reports

Vulnerability reports show you all vulnerabilities found on your system along with step by step security assessment information.

{button ,JI(`sysscan.HLP>Third`,`Export_Vulnerability_Reports_Procedure')}} [Procedure](#)

Exporting Service Reports

Service reports show you all services running on your system that are vulnerable.

{button ,JI(`sysscan.HLP>Third`,`Services_Report_Export_Procedure')}} [Procedure](#)

Exporting Trend Reports

Trend reports are used to show the history change between selected scans.

{button ,JI(`sysscan.HLP>Third`,`Trends_Report_Export_Procedure')}} [Procedure](#)

Exporting Differential Reports

Differential reports show you the differences between two scan results.

{button ,JI(`sysscan.HLP>Third`,`Exporting_Differential_Reports_Procedure')}} [Procedure](#)

{button ,AL(`reporting',0,`Main,'')} [More on reporting](#)

To Create Policies Automatically

1. From the **Policy** menu, click **New**. This opens the [New Policy Wizard](#).
2. In **Name of new policy** text box, provide the name of the new policy.
3. Under **I want the wizard to**, click **Suggest scan settings for me**.
4. Click **Next**.
5. Click **Run Smart Configuration**. The progress bar will show the completion of the smart configuration.
6. Under I want the Wizard to, click **Save the policy without modification**.
7. Click **Finish**.

To Create Policies Manually

1. From the **Policy** menu, choose **New**. This opens the [New Policy Wizard](#).
2. In **Name of new policy** text box, provide the name of the new policy.
3. Under **I want the wizard to**, click **Let me choose all scan settings for myself**.
4. Click **Next**.
5. Select the appropriate check box on the left and configure the exploits on the right.

Example

6. Click **Finish**.

To Run Scans at System Startup:

1. From the **Settings** menu, choose **General** and then click the **Basic** tab. This opens the [General Settings Dialog \(Basic\)](#) .
2. Click **Run a scan at system startup**.
3. In the **Policy to use** list, select the policy to use at system startup.
4. Click **OK**.

To Run Scans Manually:

1. Click **Scan Now**.
2. From the **Policy to use** list, select the policy.
3. Click **OK**.
4. Observe the **Overall scan progress** bar.
5. When the scan has completed, click **OK**.

Example

The Internet Protocol-FTP check box is enabled on the Left and the ftp checks are enabled on the right. The scan using this policy will only run the checked exploits.



To Run Scans at a Low Priority in the Background:

1. From the **Settings** menu, choose **General** and then click the **Basic** tab. This opens the [General Settings Dialog](#).
2. Click **Run a scan at low priority in background**.
3. From the **Policy to use** list, select the policy.
4. Click **OK**.

To Edit Policies Manually

1. From the **Policy** menu, choose **Edit**. This opens the [Edit Policy Wizard](#).
2. From the **Policy** list, select the policy to edit.
3. Click **Let me choose all scan settings for myself**.
4. Click **Next**.
5. Select the appropriate check box on the left and configure the exploits on the right.

[Detailed Configuration Example](#)

6. Click **Finish**.

To Edit Policies Automatically

1. On the **Policy** menu, click **Edit**. This opens the [Edit Policy Wizard](#).
2. In the **Policy** list, click on the policy to edit.
3. Click **Suggest scan settings for me**.
4. Click **Next**.
5. Click **Run Smart Configuration**. The progress bar will show the completion of the smart configuration.
6. Click **Save the policy without modification**.
7. Click **Finish**.

To Delete Policies:

1. From the **Policy** menu, choose **Delete**. This will open the [Delete Policy](#) Dialog.
2. Under **Policies**, select the policy to delete.
3. Click **Delete**.
4. Click **Close** or repeat steps 2 & 3 to delete additional policies.

To Rename Policies:

1. From the **Policy** menu, choose **Rename**. This will open the [Rename Policy](#) window.
2. Under **Policies**, select the policy to rename.
3. Click **Rename**.
4. Under **New policy name**, enter the new name.
5. Click **OK**.
6. Click **Close** or repeat steps 3 - 5 to rename additional policies.

To Add Schedules

1. From the **Settings** menu, choose **Schedule**. This opens the [Schedule Dialog](#).
2. Click **Add**. This opens the [Schedule Scan Dialog](#).
3. Under **Description**, enter the description of the schedule.
4. Under **Policy to use**, select a policy.
5. Under **Schedule**, set the **Frequency**, **Time**, and **Day** for the scan.
6. Click **OK**.

To Modify Schedules:

1. From the **Settings** menu, choose **Schedule**. This opens the [Schedule Dialog](#).
2. Under **Scheduled Scans**, select the schedule to modify.
3. Click **Modify**. This opens the [Schedule Scan dialog](#).
4. Under **Description**, change the description of the schedule.
5. Under **Policy to use**, select a policy.
6. Under **Schedule**, set the **Frequency**, **Time**, and **Day** for the scan.
7. Click **OK**.

To Delete Schedules:

1. From the **Settings** menu, choose **Schedule**. This opens the [Schedule Dialog](#).
2. Under **Scheduled Scans**, select the schedule to delete.
3. Click **Delete**.
4. Click **OK** when asked “Are you sure you want to delete the schedule?”
5. Click **Close**.

To Copy and Edit Policies:

1. From the **Policy** menu, click **Copy and Edit**. This opens the [Copy and Edit Policy Wizard](#).
2. In **Name of new policy** text box, provide the name of the new policy.
3. From **Policy to Copy**, select the policy to copy from.
4. Click **Next**.
5. Select the appropriate check box on the left and configure the exploits on the right.

`{button ,JI(` sysscan.HLP>Example', `Detailed_Configuration_Example')}` [Example](#)
6. Click **Finish**.

To View Vulnerability Reports:

1. From the **Report** menu, choose **Vulnerabilities**. This opens the [Vulnerabilities Report Dialog](#).
2. Under **Scans**, select the scan to report.
3. Under **Vulnerability Severity**, enable **High**, **Medium**, or **Low risk**.
4. Under **Report Detail**, enable **Full Description**, **Fix Information**, or **Policy Info**.
5. Click **Next**.
6. Click **View the report in your web browser**.
7. Click **Finish**.

To View Differential Reports:

1. From the **Report** menu, choose **Differential**. This opens the [Differential Reports Dialog](#).
2. Under **Scans**, select two scans by holding down the **CTRL** key and clicking the scans.
3. Under Differential, enable the appropriate differential option. The differential options are:
 - [Vulnerabilities in 1st scan only](#)
 - [Vulnerabilities in 2nd scan only](#)
 - [Vulnerabilities common to both](#)
4. Click **Next**.
5. Click **View the report in your web browser**.
6. Click **Finish**.

To Export Service Reports:

1. From the **Report** menu, choose **Services**. This opens the [Services Report Dialog](#).
2. Under **Scans**, select the scan to report.
3. Under **Report Detail**, enable **Full Description**, **Fix Information** , or **Policy Info**.
4. Click **Next**.
5. Click **Export the report to a file**.
6. Click **Next**.
7. (Optional) Click the **Preview** button to view the report in your browser before you save it to disk.
8. In **Name of file to export to**, enter the file name or click the **Browse** button to change the directory.
9. Click **Finish**.

To Export Trends Reports:

1. From the **Report** menu, choose **Trends...** This opens the [Trends Report Dialog](#).
2. Select one or more scans from the list by holding down the **CTRL** key and clicking the scans.
3. Click **Next**.
4. Click **Export the report to a file**.
5. Click **Next**.
6. (Optional) Click the **Preview** button to view the report in your browser before you save it to disk.
7. In **Name of file to export to**, enter the file name or click the **Browse** button to change the directory.
8. Click **Finish**.

To Export Differential Reports:

1. From the **Report** menu, choose **Differential...** This opens [Differential Reports Dialog](#)
2. Under **Scans**, select two scans by holding down the **CTRL** key and clicking the scans. Under Differential, enable the appropriate differential option. The differential options are:
 - [Vulnerabilities in 1st scan only](#)
 - [Vulnerabilities in 2nd scan only](#)
 - [Vulnerabilities common to both](#)
3. Click **Next**.
4. Click **Export the report to a file**.
5. Click **Next**.
6. (Optional) Click the **Preview** button to view the report in your browser before you save it to disk.
7. In **Name of file to export to**, enter the file name or click the **Browse** button to change the directory.
8. Click **Finish**.

To Export Vulnerability Reports:

1. From the **Report** menu, choose **Vulnerabilities**. This opens the [Vulnerabilities Report Dialog](#).
2. Under **Scans**, select the scan to report.
3. Under **Vulnerability Severity**, enable **High, Medium, or Low priority**.
4. Under **Report Detail**, enable **Full Description, Fix Information**, or **Policy Info**.
5. Click **Next**.
6. Click **Export the report to a file**.
7. Click **Next**.
8. (Optional) Click the **Preview** button to view the report in your browser before you save it to disk.
9. In **Name of file to export to**, enter the file name or click the **Browse** button to change the directory.
10. Click **Finish**.

To View Service Reports:

1. From the **Report** menu, choose **Services**. This opens the [Services Report Dialog](#).
2. Under **Scans**, select the scan to report.
3. Under **Report Detail**, enable **Full Description**, **Fix Information** , or **Policy Info**.
4. Click **Next**.
5. Click **View the report in your web browser**.
6. Click **Finish**.

To View Trend Reports

1. From the **Report** menu, choose **Trends**. This opens the [Trends Report Dialog](#).
2. Select one or more scans from the list by holding down the **CTRL** key and clicking the scans.
3. Click **Next**.
4. Click **View the report in your web browser**.
5. Click **Finish**.

Purging the Scan Results Database

1. From the **Settings** menu, choose **General**.
2. Click on the [Advanced tab](#) .
3. Under **Scan Results Database**, click **Purge Now**.
4. Verify the purge by clicking **Yes**.
5. Click **OK**.

Setting the Purge Duration

1. From the **Settings** menu, choose **General**.
2. Click on the [Advanced tab](#).
3. Under **Automatically purge scan results older than**, set the purge duration.
4. Click **OK**.

Analyzing Reports

Reports provide portability for the security assessment of your system. In addition, reports provide detailed information about vulnerabilities detected on your system, [fix](#) information for the vulnerabilities, services running, trending, and other needed information. You can [view](#) reports in your browser or [export](#) reports to standard [HTML](#) format for later analysis.

Understanding Reports

Understanding reports is the “key” to assessing vulnerabilities detected on your system, verifying services configurations, and interpreting trends for trend analysis.

{button ,JI(` sysscan.HLP>Main',` Understanding_Vuln_Rpts')} [Understanding vulnerability reports](#)
{button ,JI(` sysscan.HLP>Main',` Understanding_Service_Reports')} [Understanding service reports](#)
{button ,JI(` sysscan.HLP>Main',` Understanding_Trend_Reports')} [Understanding trend reports](#)
{button ,JI(` sysscan.HLP>Main',` Understanding_Differential_Reports')} [Understanding differential reports](#)

{button ,AL(` reporting',0,`,` Main')} [More on reporting](#)

Understanding Vulnerability Reports

Understanding the terminology in vulnerability reports is necessary for correcting the vulnerabilities. Vulnerability reports provide detailed information for each vulnerability detected on your system as well as fix information for assessment.

How to Read Vulnerability Reports

The terminology for vulnerability reports is as follows:

Vulnerability Name: The name of the vulnerability found on your system.

Severity: Severity levels for vulnerabilities are as follows:

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

Description: This describes the danger of the vulnerability on your system.

Fix: The fix is procedure based information needed to remove the vulnerability from your system.

Additional Info: This is any other information that may be useful to assess the vulnerability (e.g., [URLs](#) , Drive paths, [CERTs](#) , [RFCs](#) , etc...).

{button ,EF("hvy_vuln.html",`,`,1)} [Sample vulnerabilities reporting](#)

{button ,AL(`reporting',0,`,`Main')} [More on reporting](#)

Understanding Service Reports

Understanding the terminology in service reports is necessary for assessing misconfigured services. Service reports provide information for each service running on your system. This information includes the port of the service and port which is required by RFC. Service reports do not include vulnerability and trend information.

How to Read Service Reports

The terminology for service reports is as follows:

Services: The name of the service found.

Description: The description of the service found.

Protocol: The protocol for the service running.

Port: This is your system's port number for the service running. If this number differs from the **RFC Port** number, it is considered vulnerable.

RFC Port: This is the RFC's recommended port number for the service running. If the **Port** number is different from this number, the service is considered vulnerable.

{button ,EF("hvy_svc.html",',',1)} [Sample service report](#)

{button ,AL(`reporting',0,`,`Main')} [More on reporting](#)

Understanding Trend Reports

Understanding the terminology in trend reports is necessary for assessing security based on the history of vulnerabilities. Trend reports provide a trend analysis of your system. Trend reports document the history of vulnerabilities on your system.

How to Read Trend Reports

The terminology for trend reports is as follows:

Scan: This displays the policy used and the comment for that policy.

Date: The date shows when the scan was run on your system (date/time).

High: The number of high risk vulnerabilities found during the scan.

Medium: The number of medium risk vulnerabilities found during the scan.

Low: The number of low risk vulnerabilities found during the scan.

{button ,EF("hvy_trnds.html",`,`,1)} [Sample trend reports](#)

{button ,AL(`reporting',0,`,`Main')} [More on reporting](#)

Understanding Differential Reports

Understanding the terminology in differential reports is necessary for correcting the vulnerabilities. Differential reports compare the workstation's security vulnerabilities detected in two different scans and provide detailed information for vulnerabilities detected on the first scan, the second scan, or common to both scans. Differential reports provide fix information for assessment and do not include service and trend information

How to Read Differential Reports

The terminology for differential reports is as follows:

Vulnerabilities in First Scan Only (from High to Low severity): These are vulnerabilities that are found in the first selected scan (S1) and not in the second selected scan (S2). The formula for vulnerabilities displayed in this section is (S1 – S2).

Vulnerabilities in Second Scan Only (from High to Low severity): These are vulnerabilities that are found in the second selected scan (S2) and not in the first selected scan (S1). The formula for vulnerabilities displayed in this section is (S2 – S1).

Vulnerabilities in both scans (from High to Low severity): These vulnerabilities are common to both selected scans.

Vulnerability Name: The name of the vulnerability found on your system.

Severity: Severity levels for vulnerabilities are as follows:

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

Description

This describes the danger of the vulnerability on your system.

Fix

The fix is procedure based information needed to remove the vulnerability from your system.

Additional Info

This is any other information that may be useful to assess the vulnerability (e.g., [URLs](#) , Drive paths, [CERTs](#) , [RFCs](#) , etc...).

{button ,EF("hvy_dif.html",`,1)} [Sample differential report](#)
[Sample Applications](#)

{button ,AL(`reporting',0,`, `Main')} [More on reporting](#)

Sample Differential Report Applications

Scenario

Two heavy scans are run on your system, S1 and S2. S1 was run first and S2 second.

Differential Report Options

1. To see what new vulnerabilities have been detected since S1 was run, select S1 and S2, and generate a differential report with the “2nd scan only” option enabled.
2. To see what new vulnerabilities have been potentially fixed since S1 was run, select S1 and S2, and generate a differential report with the “1st scan only” option enabled. This shows the vulnerabilities that were present when S1 was run, but not when S2 was run.
3. To find the vulnerabilities that are still present relative to a past time (the time S1 was run), select S1 and S2, and generate a differential report with “both scans” enabled.

Purging the Scan Results Database

The [scan results database](#) is used primarily for [trend reporting](#). Purging the scan results database permanently removes all scan results from the database. You can purge the scan results database manually, at any time, or set the [purge duration](#).

Purge the Scan Results Database Now

You can purge the [scan results database](#) manually, at any time. This removes all scan results immediately.

{button ,JI(`sysscain.HLP>Third`,`Purge_the_Scan_Results_Database_Procedure`)} [Procedure](#)

Set the Purge Duration

You can set the [purge duration](#) to a specific number of days. When this number of days is reached, System Scanner automatically purges the scan results database. If you are not interested in long-term trends, set the purge duration very low (30-60 days). If you want to perform long term trend reporting, you should set the purge duration very high (3000 days maximum).

{button ,JI(`sysscain.HLP>Third`,`Set_the_Purge_Duration_procedure`)} [Procedure](#)

Resetting the Share Scan Baseline

The share scan baseline is a "snap shot" of your system's share settings. The settings include hidden shares, share permissions on an NTFS directory, permissions on the share itself, and printer share permissions. The share scan baseline is used to determine the share changes that occur on your system. If these changes are not authorized or known by a trusted user, they are considered [vulnerabilities](#).

When Should the You Reset the Share Scan Baseline?

You should reset the share scan baseline every time your share settings have changed. Share setting changes occur when you modify share permissions.

WARNING: If you fail to reset the user baseline after changing your user settings, all changes will report as [vulnerabilities](#) during the next [baseline scan](#).

{button ,JI(`sysscan.HLP>Third`,`Resetting_the_Share_Scan_Baseline_Procedure`)} [Procedure](#)

{button ,AL(`baseline`,0`,``,`Main`)} [More on baselines](#)

Resetting the Share Scan Baseline

1. From the **Policy** menu, choose [New](#), [Edit](#), or [Copy & Edit](#).
2. Enable the **Let me choose all scan settings for myself** option.
3. Click **Next**.
4. Expand the **Baselines** tree on the left side of the dialog.
5. Click **Share Scan**. Be sure that **Share Scan** is enabled.
6. On the **General** tab, click **Reset baseline scan**. If the reset box is not accessible (disabled text), then the baseline database is empty. You must [run a baseline scan](#) before resetting it.
7. Under **Select data to track**, select the [share scan options](#) to include in the baseline scan.
8. Click **Finish**.
9. Run the baseline scan to update the baseline database. Refer to [Running Scans](#).

WARNING: The file baseline database will **not** be updated until the baseline scan is run.

Resetting the User Scan Baseline

The user scan baseline is a "snap shot" of your system's user settings. The settings include logon settings, RAS settings, and user rights. The user scan baseline is used to determine the share changes that occur on your system. If these changes are not authorized or known by a trusted user, they are considered [vulnerabilities](#).

When Should the You Reset the User Baseline?

You should reset the user baseline every time your user settings have changed. User setting changes occur when you add/remove users, modify user permissions, or modify user rights.

WARNING: If you fail to reset the user baseline after changing your user settings, all changes will report as [vulnerabilities](#) during the next [baseline scan](#).

{button ,JI(` sysscan.HLP>Third', `Resetting_the_User_Baseline_Database_Procedure')} [Procedure](#)

{button ,AL(` baseline',0,`,` Main')} [More on baselines](#)

Resetting the User Scan Baseline

1. From the **Policy** menu, choose [New](#), [Edit](#), or [Copy & Edit](#).
2. Enable the **Let me choose all scan settings for myself** option.
3. Click **Next**.
4. Expand the **Baselines** tree on the left side of the dialog.
5. Click **User Scan**. Be sure that **User Scan** is enabled.
6. On the **General** tab, click **Reset baseline scan**. If the reset box is not accessible (disabled text), then the baseline database is empty. You must [run a baseline scan](#) before resetting it.
7. Under **Select data to track**, select the [user scan options](#) to include in the baseline scan.
8. Click **Finish**.
9. Run the baseline scan to update the baseline database. Refer to [Running Scans](#).

WARNING: The file baseline database will **not** be updated until the baseline scan is run.

Resetting the Group Scan Baseline

The group scan baseline is a "snap shot" of the group settings on your system. These settings include group rights and users. The Group scan baseline is used to determine the group changes that occur on your system. If these changes are not authorized or known by a trusted user, they are considered [vulnerabilities](#) .

When Should the You Reset the Group Scan Baseline?

You should reset the group scan baseline every time your group settings have changed. Group setting changes occur when you add or remove groups or modify users.

WARNING: If you fail to reset the group baseline after changing your group settings, all changes will report as [vulnerabilities](#) during the next [baseline scan](#).

{button ,JI(` sysscan.HLP>Third', `Resetting_the_Group_Scan_Baseline_Procedure')} [Procedure](#)

{button ,AL(`baseline',0,`,` Main')} [More on baselines](#)

Resetting the Group Scan Baseline

1. From the **Policy** menu, choose [New](#), [Edit](#), or [Copy & Edit](#).
2. Enable the **Let me choose all scan settings for myself** option.
3. Click **Next**.
4. Expand the **Baselines** tree on the left side of the dialog.
5. Click **User Scan**. Be sure that **User Scan** is enabled.
6. On the **General** tab, click **Reset baseline scan**. If the reset box is not accessible (disabled text), then the baseline database is empty. You must [run a baseline scan](#) before resetting it.
7. Under **Select data to track**, select the [group scan options](#) to include in the baseline scan.
8. Click **Finish**.
9. Run the baseline scan to update the baseline database. Refer to [Running Scans](#).

WARNING: The file baseline database will **not** be updated until the baseline scan is run.

Resetting the Service Baseline

The service baseline is a "snap shot" of your system's service and device settings. The settings include service applets and device applets. The service baseline is used to determine the share changes that occur on your system. If these changes are not authorized or known by a trusted user, they are considered [vulnerabilities](#).

When Should the You Reset the Service Baseline?

You should reset the service baseline every time your services and devices have changed.

WARNING: If you fail to reset the service baseline after changing your group settings, all changes will report as [vulnerabilities](#) during the next [baseline scan](#).

{button ,JI(`sysscan.HLP>Third', `Resetting_the_Service_Baseline_Procedure')}} [Procedure](#)

{button ,AL(`baseline',0,`,`Main')}} [More on baselines](#)

Resetting the Service Baseline

1. From the **Policy** menu, choose [New](#), [Edit](#), or [Copy & Edit](#).
2. Enable the **Let me choose all scan settings for myself** option.
3. Click **Next**.
4. Expand the **Baselines** tree on the left side of the dialog.
5. Click **User Scan**. Be sure that **User Scan** is enabled.
6. On the **General** tab, click **Reset baseline scan**. If the reset box is not accessible (disabled text), then the baseline database is empty. You must [run a baseline scan](#) before resetting it.
7. Under **Select data to track**, select the [service options](#) to include in the baseline scan.
8. Click **Finish**.
9. Run the baseline scan to update the baseline database. Refer to [Running Scans](#).

WARNING: The file baseline database will **not** be updated until the baseline scan is run.

Resetting the File Scan Baseline

The file scan baseline is a "snap shot" of the file configuration on your system. It is used to determine file changes that occur on your system. If these changes are not authorized or known by a trusted user, they are considered [vulnerabilities](#).

When Should You Reset the File Scan Baseline?

You should reset the baseline every time your system files have changed. System file changes occur when you add/remove software, upgrade software, or manipulate the [registry](#).

WARNING: If you fail to reset the baseline after changing your systems files, all changes will report as vulnerabilities during the next [baseline scan](#) .

{button ,JI(` sysscan.HLP>Third', `Resetting_The_File_Baseline_Database_Procedure')} [Procedure](#)

{button ,AL(`baseline',0,`,` Main')} [More on baselines](#)

Resetting the File Scan Baseline

1. From the **Policy** menu, choose [New](#), [Edit](#), or [Copy & Edit](#).
2. Enable the **Let me choose all scan settings for myself** option.
3. Click **Next**.
4. Expand the **Baselines** tree on the left side of the dialog.
5. Click **File Scan**. Be sure that **File Scan** is enabled.
6. On the **General** tab, click **Reset baseline scan**. If the reset box is not accessible (disabled text), then the baseline database is empty. You must [run a baseline scan](#) before resetting it.
7. Under **Select data to track**, select the [file scan options](#) to include in the baseline.
8. From the **Directories** tab, select the directories and files to include in the baseline.
9. From the **Extensions** tab, add extensions to include in the baseline.
10. Click **Finish**.
11. Run the baseline scan to update the baseline database. Refer to [Running Scans](#).

WARNING: The file baseline database will **not** be updated until the baseline scan is run.

Resetting the Registry Scan Baseline

The registry baseline is a "snap shot" of the registry configuration on your system. It is used to determine registry key changes that occur. If these changes are not authorized or known by a trusted user, they are considered [vulnerabilities](#) .

When Should You Reset the Registry Baseline?

You should reset the baseline every time your system's [registry keys](#) have changed. These changes occur when you add or remove software, upgrade software, or edit the registry manually by means of the registry editor ([regedt32.exe](#) for Windows NT and [regedit.exe](#) for Windows 95).

WARNING: If you fail to reset the registry baseline after changing your systems registry keys, all changes will report as [vulnerabilities](#) during the next scan.

{button ,JI(`sysscan.HLP>Third', `Resetting_the_Registry_Baseline_Procedure')} [Procedure](#)

{button ,AL(`baseline',0,`, `Main')} [More on baselines](#)

Resetting the Registry Scan Baseline

1. From the **Policy** menu, choose [New](#), [Edit](#), or [Copy & Edit](#).
2. Enable the **Let me choose all scan settings for myself** option.
3. Click **Next**.
4. Expand the Baselines tree on the left side of the dialog.
5. Click **Registry Scan**. Be sure that **Registry Scan** is enabled.
6. On the **General** tab, click **Reset baseline scan**. If the reset box is not accessible (disabled text), then the baseline database is empty. You must [run a baseline scan](#) before resetting it.
7. Under **Select data to track**, select the [registry scan options](#) to include in the baseline.
8. From the **Select** tab, enable registry keys to include in the baseline database.
9. Click **Finish**.
10. Run the baseline scan to update the baseline database. Refer to the [Running Scans](#).

WARNING: The registry baseline database will **not** be updated until [the baseline scan](#) is run.

Resetting the Process Baseline

The process baseline is a "snap shot" of your system's startup programs. The process baseline reports changes to the common Run key in registry, common Startup folder, load and run values (specify programs that are auto-started), user specific Run key in registry, and user specific Startup folder. If these changes are not authorized or known by a trusted user, they are considered [vulnerabilities](#).

When Should the You Reset the Process Baseline?

You should reset the service baseline every time your startup programs have changed and your common and specific Run keys have changed. Your Startup folder changes when you add or modify the Startup programs.

WARNING: If you fail to reset the Process baseline after changing your Startup programs, all changes will report as [vulnerabilities](#) during the next [baseline scan](#).

{button ,JI(`sysscan.HLP>Third', `Reseting_the_Process_Baseline_Procedure')}} [Procedure](#)

{button ,AL(`baseline',0,`, `Main')}} [More on baselines](#)

Resetting the Process Baseline

1. From the **Policy** menu, choose [New](#), [Edit](#), or [Copy & Edit](#).
2. Enable the **Let me choose all scan settings for myself** option.
3. Click **Next**.
4. Expand the Baselines tree on the left side of the dialog.
5. Click **Processes**. Be sure that **Processes** is enabled.
6. On the **General** tab, click **Reset baseline scan**. If the reset box is not accessible (disabled text), then the baseline database is empty. You must [run a baseline scan](#) before resetting it.
7. Under **Select data to track**, select the [process options](#) to include in the baseline.
8. From the **Select** tab, enable registry keys to include in the baseline database.
9. Click **Finish**.
10. Run the baseline scan to update the baseline database. Refer to the [Running Scans](#).

WARNING: The registry baseline database will **not** be updated until [the baseline scan](#) is run.

Share Scan Options

Enable	System Scanner
Hidden shares	tracks changes to shares that end in '\$'. There are many default, hidden shares for administration.
Permissions	tracks changes to the permissions on the directory, on a share of an NTFS directory.
Share Permissions	tracks changes to the permission of the share itself.
Printers	tracks changes to the printer shares on your system.

User Scan Options

Enable

System Scanner

Group	tracks changes to the set of groups a user belongs to.
Logon settings	tracks changes to the logon setting for the user. These are in the User Manager user details dialog.
RAS Settings	tracks changes to the RAS dialin access or call back settings. These are in the User Manager user details dialog.
User rights	tracks changes to the rights assigned to the user from the User Manager Policies . These are in the User Manager user details dialog.

Group Scan Options

Enable	System Scanner
Rights	tracks changes to the rights assigned to the user from the User Manager Policies . These are in the User Manager user details dialog.
Users	tracks changes to the user's membership.

Service Options

Enable	System Scanner
Application	tracks changes to the items in the Services applet of the control panel.
Driver	tracks changes to the items in the Devices applet of the control panel.

File Scan Options

Enable	System Scanner
Attributes	tracks changes in the attributes for files or folders.
Audit Settings (NTFS Only)	tracks changes in the auditing settings for files or folders.
Content	tracks changes in the content of files or folders.
Ownership (NTFS Only)	tracks changes in the ownership of files or folders.
Permissions (NTFS Only)	tracks changes in the permissions of files or folders.

Registry Scan Options

Enable	System Scanner
Audit Settings	tracks changes in the auditing settings for registry keys or folders.
Ownership	tracks changes in the ownership of registry keys or folders.
Permissions	tracks changes in the permissions of registry keys or folders.
Value Date	tracks changes in the value data of registry keys.

Process Options

Enable

Common Run Key in Registry

Common Startup Folder

Load

Run

User-specific Run Key in Registry

User-specific Startup Folder

System Scanner

tracks changes to the **Run** folder in the **Common** group of the **Start** menu.

tracks changes to the **Startup** folder in the **Common** group.

tracks changes to the **Load** and **Run** folders.

tracks changes to the **Load** and **Run** folders.

tracks changes in user-specific Run Keys.

tracks changes in User-specific Startup folders.

Vulnerabilities in 1st Scan Only

These are vulnerabilities that are found in the first selected scan (S1) and not in the second selected scan (S2).
The formula for vulnerabilities displayed in this section is $(S1 - S2)$.

Vulnerabilities in 2nd Scan Only

These are vulnerabilities that are found in the second selected scan (S2) and not in the first selected scan (S1).
The formula for vulnerabilities displayed in this section is (S2 - S1).

Vulnerabilities Common to Both

These vulnerabilities are common to both selected scans.

Internet Protocol Vulnerabilities

System Scanner includes the following Internet protocol checks:

- Service Scan
- FTP

Browser Vulnerabilities

System Scanner includes the following browser vulnerability checks:

- Internet Explorer
- Netscape Navigator

Operating System Vulnerabilities

System Scanner includes the following operating system vulnerability checks:

- Denial of Service
- OS Version
- IIS
- Password Settings
- Registry Settings
- User Checks
- Share Checks
- NetBIOS

Application Vulnerabilities

System Scanner includes the following application vulnerability checks:

- MS Office
- Virus Scanner
- pcANYWHERE32
- Carbon Copy 32
- Remote Possible/32
- LapLink

Baseline Vulnerabilities

System Scanner includes the following baseline vulnerability checks:

- Registry Scan
- File Scan
- Services
- Processes
- User Scan
- Group Scan
- Share Scan

Remote Access Vulnerabilities


System Scanner includes the following remote access checks:

- Modems
- RAS

To Stop Scans:

From the File menu, choose Stop Scan.


-OR-

On the main window, click .

To Pause Scans:

From the File menu, choose Pause Scan.


-OR-

On the main window, click 

To Resume Scans

From the File menu, choose Pause Scan.

-OR-

On the main window, click 

To Secure the Installation Directory:

1. From the **Settings** menu, choose **General**.
2. Click the **Advanced** tab.
3. Enable the check box for **Have scans verify that the SysScan install directory is secure**.
4. Click **OK**.

To Resetting the Baseline(s):

1. From the **Policy** menu, choose **Reset Baselines**. This opens the [Reset Baseline Dialog](#)
2. Under **Policy**, select the [policies](#) to modify.
3. Under **Baselines**, enable the checkbox for each baseline to reset.
4. Click one of the following:

Button	Functionality
Reset	Resets the selected baselines
Close	Closes this dialog.

System Scanner Command Line (SSCLI)

What can you do?

With the [SSCLI](#) , you can:

- Run a scan
- Run a report
- Refresh the schedule

About SSCLI parameters

All of the [SSCLI parameters](#) are either optional or conditional. You must either run a scan, run a report, or refresh the schedule (or some combination of these).

NOTE: The parameters are **not** case-sensitive.

{button ,AL(`sscli parameters',0,`,`>Main')}} [More on SSCLI parameters](#)

To use the Command Line

1. From the Start menu, choose Run.
2. Type: cmd.
3. Click OK. The command line window opens
4. Use a combination of the [SSCLI parameters](#) to scan, schedule, or report.
5. Press Enter.

Examples of SSCLI Parameter Commands

Example of running a scan

Below is an example of running a heavy scan:

```
sscli -p heavy
```

Example of running a report

You do not need to specify any report options. System scanner uses the default options of the report wizards and any options that are not applicable to a particular report type will be ignored (e.g., options 1 and 2 will be ignored unless the report type is Differential). Below is an example of running a report:

```
sscli -p heavy -r v -f "e:\reports\vuln.htm"
```

Example of refreshing a schedule

Below is an example of refreshing a schedule:

```
sscli -noscan -sched
```

{button ,AL(`sscli parameters',0,`,`>Main')} [More on SSCLI parameters](#)

Default Policy Groups

Policies have been grouped into the following three classes:

[Server Policies](#)

[User Desktop System Policies](#)

[Technical Policies.](#)

The policy names have been modified to allow a sorting by type, by prepending the term "Server - ", "User - ", or "Technical - " to the beginning of the policy name.

Note: An exhaustive list of checks that is enabled by each policy is **not** provided. The granularity provided by the policy editor is such that groups of checks are frequently all enabled, or not enabled at all.

{button ,AL(` policies',0,`,`Main')}} [More on default policies](#)

Server Policies

These policies are intended for use on systems that provide important services to an organization. Depending on the type of system and its deployment, many checks can be enabled.

NOTE: These policies are installed on Microsoft Windows NT only.

The Server Policies are:

- [Server-DMZ FTP or Mail Server](#)
- [Server-DMZ Web Server](#)
- [Server – Intranet Server](#)
- [Server – Departmental Server](#)

{button ,AL(` policies',0,`,`, ` Main')}` [More on default policies](#)

User Desktop System Policies

These policies are intended for use on end-user desktop systems. Because these computers are typically less critical to the organization, fewer checks are enabled than for server policies.

The User Desktop System Policies are:

- [User – Power User Desktop Workstation](#)
- [User – Desktop Workstation](#)
- [User - Home Computer](#)

{button ,AL(` policies',0,`,`, ` Main') } [More on default policies](#)

Technical Policies

These policies enable particular types of checks. These policies might have wide applicability, or be interesting for investigating specific issues across the entire enterprise (e.g. “Which systems do not have virus scanners installed?” or “Which systems have modems installed?”).

- [Technical – Baselines Policy](#)
- [Technical – Browser Only Policy](#)
- [Technical – Heavy Scan Policy](#)
- [Technical – OS Lockdown Policy](#)
- [Technical – Services Scan Policy](#)

{button ,AL(` policies',0,`,` Main')}} [More on default policies](#)

To open file system properties:

1. Open Windows NT Explorer.
2. Navigate to the directory or file indicated in the vulnerability fix information.
3. Right click on the directory or file.
4. Choose Properties, Security.

To start the Registry Editor program:

1. From the Start menu, click Run.
2. Type one of the following:

IF you have this Operating System	THEN Type this...
Windows 95	regedit
Windows 98	
Windows NT	regedt32

3. Click OK.
4. Click the window name that corresponds to the registry key you need to view or edit. For example, click the HKEY_LOCAL_MACHINE window to work with a key or value in that hierarchy.

To apply the latest Windows NT Service Pack:

1. Open a web browser.
2. Go to <http://support.microsoft.com/support/ntserver/Content/ServicePacks/> and follow the directions to download the appropriate service pack for your computer.
3. Find the installation program you downloaded to your computer.
4. Double-click the program icon to start the installation.
5. Follow the installation directions.

To start the User Manager program:

1. From the Start menu, click Programs.
2. Point to Administrative Tools (Common).
3. Click User Manager. The User Manager main window appears.

Opening the Policy Editor

1. From the Start menu, choose Programs, Policy Editor. The Policy Editor main window appears.
2. From the File menu, choose Open Registry.

To restart inetd:

1. Go to a command line.
2. Type `kill -HUP pid`, where *pid* is the inetd's process ID number.

Telnetd Environment Workaround

This information is from CERT Advisory CA-95:14 "Telnetd Environment Vulnerability," Appendix B at ftp://ftp.cert.org/pub/cert_advisories/CA-95:14.Telnetd_Environment_Vulnerability.

```
/*
 * This is a login wrapper that removes all instances of
 * various variables from the environment.
 *
 * Note: this program must be compiled statically to be
 * effective against exploitation.
 *
 * Author: Lawrence R. Rogers
 *
 * 10/25/95 version 1.1 Original version
 * 10/26/95 version 1.2 ELF_ variables removed (Linux)
 * 10/27/95 version 1.3 ELF_ changed to ELF_LD_
 * Added AOUT_LD_ (Linux)
 */
#include <stdio.h>
#if !defined(_PATH_LOGIN)
# define _PATH_LOGIN "/bin/login.real"
#endif
main (argc, argv, envp)
int argc;
char **argv, **envp;
{
    register char **p1, **p2;
    for (p1 = p2 = envp; *p1; p1++) {
        if (strncmp(*p1, "LD_", 3) != 0 &&
            strncmp(*p1, "_RLD", 4) != 0 &&
            strncmp(*p1, "LIBPATH=", 8) != 0 &&
            strncmp(*p1, "ELF_LD_", 7) != 0 &&
            strncmp(*p1, "AOUT_LD_", 8) != 0 &&
            strncmp(*p1, "IFS=", 4) != 0 ) {
                *p2++ = *p1;
        }
    }
    *p2 = 0;
    execve(_PATH_LOGIN, argv, envp);
    perror(_PATH_LOGIN);
    exit(1);
}
```

The following two examples show how to compile the login-wrapper for SGI's IRIX 5.3 and FreeBSD 2.x systems. The examples move the distributed login program to a new location and install the wrapper in the standard location. When executed, the wrapper first cleanses the environment and then calls the relocated, distributed login program.

Note 1: The wrapper must be compiled statically. On SGI's IRIX system, compiling statically requires that the non-shared versions of libraries be installed. Consult your system documentation to determine how to do this.

Note 2: You may need to change the `_PATH_LOGIN` variable to define where the real login program resides on your system. On some systems, login resides in `/usr/bin/login`.

Compiling for IRIX 5.3:

```
# uname -a
IRIX test 5.3 11091812 IP22 mips
# /bin/ls -l /usr/lib/iaf/scheme
- -rwsr-xr-x 1 root sys 65832 Sep 9 14:24 /usr/lib/iaf/scheme
# /bin/cc -non_shared -O -D_PATH_LOGIN=\"/usr/lib/iaf/scheme.real\" \
login-wrapper.c -o login-wrapper
# /bin/mv /usr/lib/iaf/scheme /usr/lib/iaf/scheme.real
# /bin/chmod 755 /usr/lib/iaf/scheme.real
# /bin/mv login-wrapper /usr/lib/iaf/scheme
# /bin/chmod 4755 /usr/lib/iaf/scheme
# /bin/chown root /usr/lib/iaf/scheme
# /bin/chgrp sys /usr/lib/iaf/scheme
# /bin/ls -lL /usr/lib/iaf/scheme /usr/lib/iaf/scheme.real
- -rwxr-xr-x 1 root sys 65832 Sep 9 14:24
/usr/lib/iaf/scheme.real
```

```
- -rwsr-xr-x 1 root sys 213568 Oct 30 08:42 /usr/lib/iaf/scheme
```

Compiling for FreeBSD 2.x:

```
# /bin/ls -lg /usr/bin/login
- -r-sr-xr-x 1 root bin 20480 Jun 10 20:00 /usr/bin/login
# /usr/bin/cc -D_PATH_LOGIN=\"/usr/bin/login.real\" -static \
    -O login-wrapper.c -o login-wrapper
# /bin/mv /usr/bin/login /usr/bin/login.real
# /bin/chmod 555 /usr/bin/login.real
# /bin/mv login-wrapper /usr/bin/login
# /bin/chmod 4555 /usr/bin/login
# /usr/sbin/chown root.bin /usr/bin/login
# /bin/ls -lg /usr/bin/login /usr/bin/login.real
- -r-sr-xr-x 1 root bin 24885 Oct 25 22:14 /usr/bin/login
- -r-xr-xr-x 1 root bin 20480 Jun 10 20:00 /usr/bin/login.real
```


To restart a service in Windows NT:

1. [Open the Services control panel.](#)
2. Select the service.
3. Click Stop.
4. When the service has stopped, click Start.
5. Click OK.

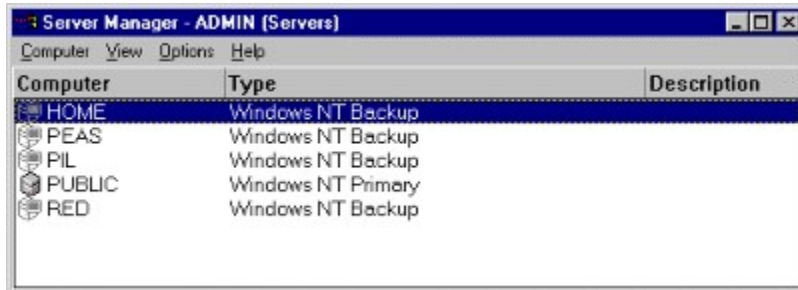
To stop or disable a service in Windows NT:

- 1 [Open the Services control panel](#). To open the Services control panel, >(w95sec)
- 2 Select the service.
- 3 Click Stop.
- 4 When the service has stopped, click Startup.
- 5 Choose one of these options:
 - To permanently disable the service, click Disabled.
 - To turn the service off unless manually activated by the user or a program, click Manual.
- 6 Click OK, then click Close.

To start Server Manager:

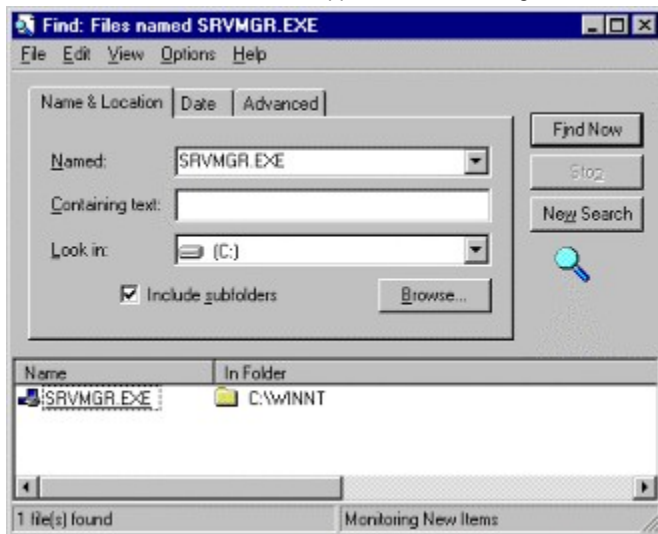
Server Manager is a utility installed with Windows NT Server 4.0. It can also run on Windows NT Workstation, but must be installed separately. See [To Install Server Manager](#) if you cannot locate Server Manager on your machine.

1. From the Start menu, click Programs.
2. Point to Administrative Tools (Common).
3. Click Server Manager. The Server Manager main window appears.



Note: If Server Manager was installed separately from the operating system, search for and run SRVMGR.EXE:

1. From the Start Menu, click Find, then click Files or Folders.
2. The Find All Files window appears. The following window shows suggested settings and the search outcome.



3. In the Named field, type SRVMGR.EXE.
4. Verify that the drive letter in the Look in field corresponds to the drive containing your WINNT directory.
5. Verify that Include subfolders is checked.
6. Click Find Now.
7. Double click the file name that appears in the Name column.

To Install Server Manager:

1. From your web browser, go to Microsoft Support Online and download “SRVTOOLS.EXE: Windows NT 4.0 versions of User Manager and Server Manager” at <http://support.microsoft.com/download/support/mslfiles/SRVTOOLS.EXE>. This file is approximately 393K. More information on the Server Tools is available at <http://support.microsoft.com/support/kb/articles/Q173/6/73.asp>.
2. For Microsoft Internet Explorer, the File Download window appears. Click Save this program to disk and click OK.
3. Select a location to save the Server Tools installation file.
4. After the download is complete, run the installation file you saved in the previous step.
5. Four files are created in the directory that contains the installation file: SRVMGR.EXE, SRVMGR.HLP, USRMGR.EXE, and USRMGR.HLP. You can run SRVMGR.EXE from the current folder, or move these files to another folder.

To open the Services control panel:

- 1 From the Start menu, point to Settings, then choose Control Panel. The Control Panel window appears.
- 2 Choose Services from the list of icons in the Control Panel window. The Services control panel appears.

To Disable A Unix Daemon started from inetd:

- 1 Edit the /etc/inetd.conf (or equivalent) file.
- 2 Locate the line that controls the daemon.
- 3 Type a # at the beginning of the line to comment out the daemon.
- 4 [Restart inetd](#). To_restart_inetd_>(w95sec)

To open the Network control panel:

- 1 From the Windows NT Desktop, right click Network Neighborhood. The Network control panel appears.

To remove a share from a remote computer:

- 1 From a remote computer, [open the Server Manager](#).
- 2 Select the host name.
- 3 From the Computer menu, choose Shared Directories. The Shared Directories window appears.
- 4 Select the NetBIOS share
- 5 Choose Stop Sharing.

To remove a share from a local computer:

- 1 From the local computer, [open Windows NT Explorer](#).
- 2 Navigate to the shared folder.
- 3 Right-click the shared folder name and select Sharing.
- 4 To disallow access to all users, choose Not Shared.

To remove a share from the command line:

From a command prompt, type `net share sharename /delete.`

To grant share access to authorized users:

- 1 From the local computer, [open Windows NT Explorer](#).
- 2 Navigate to the shared folder.
- 3 Right-click the shared folder name and select Sharing.
- 4 Click Permissions.
- 5 Use these guidelines to review the listed permissions:
 - Remove or change any permissions such as Everyone – Full Control. This default permission allows all users to read, modify, and even change ownership and permissions on the items in the share.
 - Review any names with Change or Full Control permissions and determine if the permission is appropriate. Consider using Read Only or No Access if these names do not need to modify items in the share.
 - Review any names that should not be in the list, and remove the name or change their permission as appropriate.

To set access to the Windows NT repair folder from the command line:

Note: This example assumes that your %SystemRoot% folder is C:\winnt. You may need to change this value depending on the location of %SystemRoot%.

From the command line, type these two commands:

```
cacls c:\winnt\repair /g administrators:F  
cacls c:\winnt\repair /g system:F
```

To disable a Windows NT user account:

- 1 [Open the User Manager.](#)
- 2 Select the user account.
- 3 From the User menu, select Properties.
- 4 Choose Account Disabled.
- 5 Click OK.

To implement user-specific permissions in Windows 95:

If disabling Windows 95 sharing is unacceptable, you can use user-level access control. This approach does not eliminate reporting for a vulnerability, but it does decrease the risk. Windows 95 permits user-specific permissions if it is part of a domain. Access to the share by password is discouraged because of the possibility of unlimited and unlogged [brute force](#) attacks. To implement user-specific permissions:

- 1 [Open the Network control panel](#). To open the Network control panel_>(w95sec)
- 2 From the Access Control page, choose User-Level access control.
- 3 Type the domain name.
- 4 Click OK.

To remove file and print sharing from Windows 95:

- 1 [Open the Network control panel.](#)
- 2 From Configuration, click File and Print Sharing.
- 3 Disable 'I want to be able to give others access to my files.'
—AND—
Disable 'I want to be able to allow others to print to my printer(s).'
- 4 Click OK and restart the computer. The Windows 95 machine no longer allows shares to exist or be created.

To remove login access for a Unix account:

- 1 Edit the `/etc/passwd` file.
- 2 Locate the account.
- 3 Place an `*` (asterisk) in the password field.
- 4 Place the string `/bin/false` in the shell field.
- 5 An example of the `/etc/passwd` entry for a disabled guest account should resemble the following:
`guest:*:2311:50:Guest User:/home/guest:/bin/false`
- 6 Save and exit the file.

To disable login access to a Windows account:

- 1 Open [User Manager](#). To_start_the_User_Manager_program>(w95sec)
- 2 Double click the account. The User Properties dialog appears.
- 3 To disable the account, select the Account Disabled check box.
- 4 Choose OK.

To change a password on a Windows account:

- 1 Open [User Manager](#). To start the User Manager program >(w95sec)
- 2 Double click the account. The User Properties dialog appears.
- 3 To change the password to something difficult to guess, type and confirm the new password.
- 4 Choose OK.

To identify and remove public community names from Windows SNMP:

Detailed information is available from the Microsoft Knowledge Base article “How to: Configure SNMP security” at <http://support.microsoft.com/support/ntserver/serviceware/10140298.asp>.

- 1 [Open the Network control panel.](#)
- 2 Click the Services tab.
- 3 Click SNMP Service.
- 4 Click Properties.
- 5 Click the Security tab.
- 6 Verify that your configuration contains the following secure settings:
 - At least one Accepted Community Name exists. Empty lists cause SNMP to accept requests from anyone. (See Microsoft Knowledge Base article Q99880, “How to: Configure SNMP security” at <http://support.microsoft.com/support/kb/articles/q99/8/80.asp>.)
 - The Accepted Community Names are *not* default or easily guessed names, such as public.
 - The Only Accept SNMP Packets from These Hosts option is selected, and one or more IP Host or IPX address are specified.
 - Each host and community name in the lists is a valid destination.
- 7 In addition to securing SNMP from the control panel, you will want to secure it from the Registry.

To restrict anonymous connections in Windows NT:

WARNING: Incorrectly using Registry Editor may cause severe and irreparable damage and may require you to reinstall your operating system. Internet Security Systems cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

- 1 If you have not already done so, [apply Windows NT 4.0 Service Pack 3](http://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP2/sec-fix/) or the post-SP2 sec-fix patch available at [ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP2/sec-fix/](http://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP2/sec-fix/) .
- 2 [Open the Registry Editor.](#)
- 3 Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA.
- 4 From the Edit menu, choose Add Value. The Add Value window appears.
- 5 In the Value Name field, type `RestrictAnonymous`.
- 6 Select REG_DWORD as the Data Type.
- 7 Click OK. The DWORD Editor appears.
- 8 In the Data field, type 1. (Ignore the Radix setting.)
- 9 Click OK. Registry Editor adds the key to the registry.
- 10 Reboot the system to apply the changes.

Note: Changing the Registry entries is only effective after the post-SP2 sec-fix patch or Service Pack 3 have been applied.

To open the Event Viewer:

- 1 From the Start menu, click Programs, then point to Administrative Tools, then choose Event Viewer. The Event Viewer window appears.
- 2 From the Log menu, select one of these options:
 - System. The System log records events logged by the Windows NT system components. For example, the failure of a driver or other system component to load during startup is recorded in the System log.
 - Security. The Security log records security events. This log helps track changes to the security system and identifies any possible breaches to security. For example, attempts to log on the system may be recorded in the Security log, depending on the Audit settings in User Manager. You can view the Security log only if you are an Administrator for a computer.
 - Application. The Application log records events logged by applications. For example, a database application might record a file error in the Application log.

To rename the Administrator account:

- 1 [Open the User Manager.](#)
- 2 Select the Administrator account.
- 3 From the User menu, select Rename. The Rename window appears.
- 4 Change the name of the Administrator account and click OK.

To create a new Administrator account and assign it to the Guest group:

- 1 [Open the User Manager.](#)
- 2 From the User menu, select New User. The New User window appears.
- 3 Add a new user named Administrator, with a non-trivial password. Non-trivial_password>(w95sec)
- 4 Click Groups. The Group Memberships window appears.
- 5 Verify Administrator is only a member of the Guest group. Click OK twice to close both the Group Memberships and New User windows.

To implement System Event Auditing:

- 1 [Open the User Manager.](#)
- 2 Select the user account.
- 3 From the Policies menu, select Audit. The Audit Policy window appears.
- 4 Choose Audit these events. The audit choices are enabled.
- 5 From the Restart, Shutdown, and System field, click Failure or Success as indicated on the NT Auditing/Misc policy page. Click OK.

To implement Logon and Logoff Auditing:

- 1 [Open the User Manager.](#)
- 2 Select the user account.
- 3 From the Policies menu, select Audit. The Audit Policy window appears.
- 4 Choose Audit these events. The audit choices are enabled.
- 5 From the Logon and Logoff field, click Failure or Success as indicated on the NT Auditing/Misc policy page. Click OK.

To implement File and Object Access Auditing at the system level:

- 1 [Open the User Manager.](#)
- 2 Select the user account.
- 3 From the Policies menu, select Audit. The Audit Policy window appears.
- 4 Choose Audit these events. The audit choices are enabled.
- 5 5 From the File and Object Access field, click Failure or Success as indicated on the NT Auditing/Misc policy page. Click OK.

Note: File and Object Access auditing will produce numerous log entries, most of which are benign. In addition, auditing several objects can degrade system performance. Auditing only occurs on objects that have been marked for auditing. To audit events, follow the procedure in [To implement File and Object Access Auditing at the object level](#) .

To implement File and Object Access Auditing at the object level:

Note: This auditing will produce numerous log entries, most of which are benign. In addition, auditing several objects can degrade system performance. To track these accesses, File and Object Access auditing must be enabled at the system level. See [To implement File and Object Access Auditing at the system level](#) for more information.

- 1 Using My Computer or Windows NT Explorer, go to the object that you want to audit.
- 2 Right click the object and select Properties.
- 3 Select the Security tab.
- 4 Click Auditing. The File Auditing, Directory Auditing, or Printer Auditing dialog appears.
- 5 Select one of these choices:
 - To add a new user or group name, click Add. [Add the names from the Add Users and Groups dialog.](#)
 - To modify auditing, select the name and the Success and Failure audits that are required for your security policy.
 - To remove auditing, select the name and click Remove.
- 6 Click OK twice to apply the changes.

To implement Restart, Shutdown, and System auditing:

- 1 [Open the User Manager.](#)
- 2 Select the user account.
- 3 From the Policies menu, select Audit. The Audit Policy window appears.
- 4 Choose Audit these events. The audit choices are enabled.
- 5 From the Restart, Shutdown and System field, click Failure or Success as indicated on the NT Auditing/Misc policy page. Click OK.

To implement Use of User Rights auditing:

- 1 [Open the User Manager.](#)
- 2 Select the user account.
- 3 From the Policies menu, select Audit. The Audit Policy window appears.
- 4 Choose Audit these events. The audit choices are enabled.
- 5 From the Use of User Rights field, click Failure or Success as indicated on the NT Auditing/Misc policy page. Click OK.

To implement Process Tracking:

- 1 [Open the User Manager.](#)
- 2 Select the user account.
- 3 From the Policies menu, select Audit. The Audit Policy window appears.
- 4 Choose Audit these events. The audit choices are enabled.
- 5 From the Process Tracking field, click Failure or Success as indicated on the NT Auditing/Misc policy page. Click OK.

To implement Security Policy Changes auditing:

- 1 [Open the User Manager.](#)
- 2 Select the user account.
- 3 From the Policies menu, select Audit. The Audit Policy window appears.
- 4 Choose Audit these events. The audit choices are enabled.
- 5 From the Security Policy Changes field, click Failure or Success as indicated on the NT Auditing/Misc policy page. Click OK.

To implement User and Group Management auditing:

- 1 [Open the User Manager.](#)
- 2 Select the user account.
- 3 From the Policies menu, select Audit. The Audit Policy window appears.
- 4 Choose Audit these events. The audit choices are enabled.
- 5 From the User and Group Management field, click Failure or Success as indicated on the NT Auditing/Misc policy page. Click OK.

To prevent remote logon of a Windows NT user account:

- 1 [Open the User Manager.](#)
- 2 Select the user account.
- 3 From the Policies menu, choose User Rights.
- 4 In the Right field, choose Access this computer from network.
- 5 In the Grant To field, highlight the user account and click Remove.

To assign a non-trivial password in Windows NT:

- 1 [Open the User Manager.](#)
- 2 Select the user account.
- 3 From the Policies menu, select Account.
- 4 For the Minimum Password Length, require a minimum length of at least 6 characters. Click OK.
- 5 From the User menu, select Properties. The User Properties window appears.
- 6 Type and confirm a [non-trivial password.](#) Click OK.

To change the minimum password length:

- 1 [Open the User Manager.](#)
- 2 From the Policies menu, choose Account. The Account Policy window appears.
- 3 Set the minimum password length to at least the number of characters specified by the current Internet Scanner policy. Click OK.

To change the password history value:

- 1 [Open the User Manager.](#)
- 2 From the Policies menu, choose Account. The Account Policy window appears.
- 3 In the Password Uniqueness box, set the value to remember to at least the value specified by the current Internet Scanner policy. Click OK.

To change the minimum password age:

- 1 [Open the User Manager.](#)
- 2 From the Policies menu, choose Account. The Account Policy window appears.
- 3 In the Minimum Password Age box, set the Expires In value to at least the value specified by the current Internet Scanner policy. Click OK.

To change the maximum password age:

- 1 [Open the User Manager.](#)
- 2 From the Policies menu, choose Account. The Account Policy window appears.
- 3 In the Maximum Password Age box, set the Allow Changes In value to at most the value specified by the current Internet Scanner policy. Click OK.

To enable forced logoffs in Windows NT Server:

- 1 [Open the User Manager.](#)
- 2 Select the user account.
- 3 From the Policies menu, choose Account. The Account Policy window appears.
- 4 Choose Forcibly Disconnect Remote Users From Server When Logon Hours Expire. This option is visible only when the server is a Primary Domain Controller. Click OK.

To change the account lockout count:

- 1 [Open the User Manager.](#)
- 2 From the Policies menu, choose Account. The Account Policy window appears.
- 3 Enable Account Lockout.
- 4 Set the Lockout After n bad logon attempts to a value that is less than or equal to the value in the current Internet Scanner policy. Click OK.

To change the account lockout reset time:

- 1 [Open the User Manager.](#)
- 2 From the Policies menu, choose Account. The Account Policy window appears.
- 3 Enable Account Lockout.
- 4 Set the Reset count After n minutes to a value that is less than or equal to the value in the current Internet Scanner policy. Click OK.

To change the account lockout duration:

- 1 [Open the User Manager.](#)
- 2 From the Policies menu, choose Account. The Account Policy window appears.
- 3 Enable Account Lockout.
- 4 Set the Duration field to a value that is less than or equal to the value in the current Internet Scanner policy. Click OK.

To remove a network service from Windows NT

- 1 [Open the Network control panel.](#)
- 2 Choose the Services tab.
- 3 Highlight the service you want to remove.
- 4 Click Remove and confirm the removal.
- 5 Click OK to close the Network control panel.

To remove a network protocol from Windows NT:

- 1 [Open the Network control panel.](#)
- 2 Choose the Protocols tab.
- 3 Highlight the network protocol you want to remove.
- 4 Click Remove and confirm the removal.
- 5 Click OK to close the Network control panel.

To restrict anonymous connections from listing account names:

- 1 [Open the Registry Editor.](#)
- 2 Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA.
- 3 From the Edit menu, choose Add Value. The Add Value window appears.
- 4 Type a Value Name of RestrictAnonymous with Data Type: REG_DWORD. Click OK. The DWORD Editor window appears.
- 5 Type the number 1 in the Data field. Leave the Radix value at the current setting.
- 6 Click OK and exit the Registry Editor.
- 7 Reboot the system to apply the changes.

To install the password filter:

The password filter (at %system root%\SYSTEM32\PASSFILT.DLL) should be copied to the primary domain controller for the domain, and to any backup domain controllers in the event the server role in the domain changes. To use the password filter, the Notification Packages registry entry must exist. If it doesn't exist, then you must create it.

WARNING: Incorrectly using Registry Editor may cause severe and irreparable damage and may require you to reinstall your operating system. Internet Security Systems cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

- 1 [Open the Registry Editor.](#)
- 2 Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.
- 3 From the Edit menu, choose Add Value. The Add Value window appears.
- 4 Type a Value Name of Notification Packages with Data Type REG_MULTI_SZ. Click OK. The Multi-String Editor appears.
- 5 In the Data field, type Passfilt.dll

Notification Packages contains a list of DLLs to be loaded and notified of password changes and password change requests. You can audit the loading of Notification Packages by setting the audit policy in User Manager. To do this, start User Manager and then click Audit on the Policies menu. In the Audit Policy dialog box click Audit These Events and then enable Restart, Shutdown, and System by selecting the Success and/or Failure check boxes.

Passfilt.dll implements the following password policy:

- § § Passwords must be at least 6 characters long.
- § § Passwords must contain characters from at least 3 of the following 4 classes:
 - English Upper Case Letters A, B, C, ... Z
 - English Lower Case Letters a, b, c, ... z
 - Westernized Arabic Numerals 0, 1, 2, ... 9
 - Non-alphanumeric characters .,:*&%!
- § § Passwords may not contain your user name or any part of your full name.

Custom password filter DLLs can be written to implement different password rules. For more information, see Microsoft Knowledge Base article Q151082 "Password Change Filtering & Notification in Windows NT" at <http://support.microsoft.com/support/kb/articles/q151/0/82.asp>.

To restrict registry access:

- 1 [Open the Registry Editor.](#)
- 2 Go to the key that requires permissions.
- 3 From the Security menu, choose Permissions. The Registry Key Permissions window appears.
- 4 Use these guidelines to review the listed permissions:
 - Remove or change any permissions such as Everyone – Full Control. This default permission allows all users to read, modify, and even change ownership and permissions on the items in the share.
 - Review any names with Full Control permissions and determine if the permission is appropriate. Consider using Special Access, Read, or removing permissions if these names do not need to modify items in the key.
 - Review any names with Special Access permissions and determine if the permission is appropriate. Consider using Read or removing permissions if these names do not need to modify items in the key.
 - Review any names that should not be in the list, and remove the name or change their permission as appropriate.

To restrict access to the Windows repair directory:

- 1 [Open Windows NT Explorer.](#)
- 2 Go to the %systemroot\repair subdirectory. This subdirectory is usually located in the \winnt or \windows directory.
- 3 Right click the repair directory and choose Sharing. The repair Properties window appears on the Sharing page.
- 4 Verify that Shared As is selected.
- 5 Click Permissions.
- 6 If Everyone – Full Control is present, highlight the name and click Remove.
- 7 Click Add. The Add Users and Groups window appears.
- 8 [Select the Administrators group and other users who need administrator access.](#)
- 9 For the Type of Access, choose Full Control.
- 10 Click OK three times to return to Windows NT Explorer.

To open Windows NT Explorer:

- 1 From the Start menu, click Programs.
- 2 Click Windows NT Explorer.

What to do if a computer's security is compromised:

- 1 *Immediately* remove the computer from the network.
- 2 Create a backup of the contents of the hard drive, or isolate the data on a non-networked storage device.
- 3 Perform a low-level format of all hard drives on the computer.
- 4 Reinstall the operating system.
- 5 Configure the computer with the original user names, groups, and applications.
- 6 Run Internet Scanner to determine vulnerabilities, and resolve detected vulnerabilities.
- 7 Before using the files on the backup, scan all files using an up-to-date antivirus program, and copy only the files you know to be authorized on that computer.
- 8 Reconnect the computer to the network.

To disable FPNWCLNT.DLL:

- 1 [Open the Registry Editor](#).To_open_the_registry_editor_(w95sec)
- 2 Go to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
- 3 Double click the Notification Packages value.
- 4 If the FPNWCLNT string is present, highlight and delete it.

To fortify SNMP registry entries:

- 1 [Open the Registry Editor.](#)
- 2 Go to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents key.
- 3 Highlight the SOFTWARE\Microsoft\LANManagerMIB2Agent\CurrentVersion value.
- 4 From the Edit menu, select Delete. Click Yes to confirm the deletion of this value.

To disable autologon in Windows NT:

- 1 [Open the Registry Editor.](#)
- 2 Go to the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon key.
- 3 Select the AutoAdminLogon value.
- 4 From the Edit menu, select Delete. Click Yes to confirm the deletion of this value.
- 5 Repeat steps 3 and 4 for the DefaultUser and DefaultPassword registry values.

To associate the .reg file name extension in Windows 95:

In Windows 95, an error causes existing file associations changed from the File Types dialog box to revert to another value. Therefore, complete one of the following procedures:

§ § From the File Types dialog box, [remove the existing association](#).

Then [create a new .reg file association to a text editor, such as Notepad or Wordpad](#).

§ § Change the .reg file association from the Registry Editor. This option is simpler, but involves more risk for inexperienced users. If you are uncomfortable making changes to the registry, use the first option.

WARNING: Incorrectly using Registry Editor may cause severe and irreparable damage and may require you to reinstall your operating system. Internet Security Systems cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

To change the .reg file association from the registry editor:

- 1 [Open the Registry Editor.](#)
- 2 Go to the HKEY_LOCAL_MACHINE/Software/Classes/regfile/shell/open/command key.
- 3 Double click the value that is similar to <No Name> : REG_SZ : regedit.exe %1. The String Editor window appears.
- 4 Change the regedit.exe entry to notepad.exe. Do not alter any other portion of the string.
- 5 Click OK.

To remove an existing .reg file association:

- 1 Open My Computer.
- 2 From the View menu, select Folder Options.
- 3 Select the File Types tab.
- 4 In the registered file types list, locate and select Registration Entries.
- 5 Click Remove. Confirm the removal by selecting Yes.

To create a new .reg file association:

- 1 Open My Computer.
- 2 Locate a spare file on a local drive and rename the extension to .reg. Do not use an existing .reg file, because the next steps will cause it to be executed.
- 3 Open the file you just renamed.
- 4 One of the following situations will occur:
 - If the Registry Editor starts, then the old association still exists. [You must first remove this association before continuing.](#)
 - If a text editor program starts and displays the contents of the .reg file, then the association is already correct. You do not need to continue this procedure.
 - If the Open With window appears, then select a program such as NOTEPAD or WORDPAD.
- 5 In the Description field, type `Registration Entries`.
- 6 Verify that the 'Always use this program to open this file' is enabled.
- 7 Click OK.

To associate the .reg file name extension in Windows NT:

[These changes can also be made from the Registry Editor.](#) However, incorrectly using Registry Editor may cause severe and irreparable damage and may require you to reinstall your operating system. Internet Security Systems cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

- 1 Open My Computer.
- 2 From the View menu, select Folder Options.
- 3 Select the File Types tab.
- 4 In the registered file types list, locate and select Registration Entries.
- 5 Click Edit.
- 6 In the Actions list, click the first action.
- 7 Click Edit.
- 8 Change all references of regedit.exe to a text editor, such as notepad.exe or wordpad.exe.
- 9 Click OK, then click Close twice to apply the changes.

To clear the Windows NT paging file at shutdown:

- 1 [Open the Registry Editor.](#)
- 2 Go to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management key.
- 3 Double click the ClearPageFileAtShutdown value. The DWORD Editor window appears.
- 4 Change the Data value to 1 and click OK.

To specify Windows NT authentication:

- 1 [Open the Registry Editor.](#)
- 2 Go to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\LSA key.
- 3 Select one of the following choices:
 - If the LMCompatibilityLevel value does not exist, go to the Edit menu and select Add Value. Type the following information in the Add Value window, then click OK:
Value Name: LMCompatibilityLevel
Value Type: REG_DWORD
 - If the LMCompatibilityLevel value exists, double click the entry and go to the next step.
- 4 In the DWORD Editor window, set the Data field to 1 (Send Windows NT authentication and LM authentication only if the server requests it) or 2 (Never send LM authentication).
Note: If a Windows NT client selects 2, it cannot connect to servers that support only LM authentication, such as Windows 95 and Windows for Workgroups.
- 5 Click OK.

To disable DCOM:

- 1 From the Start menu, select Run.
- 2 Type dcomcnfg to display the Distributed COM Configuration Properties window.
- 3 Click Default Properties.
- 4 Clear Enable Distributed COM on this computer.
- 5 Click OK.

To secure DCOM from the registry:

- 1 [Open the Registry Editor.](#)
- 2 Go to the HKEY_LOCAL_MACHINE/Software/Microsoft/Ole key.
- 3 From the Security menu, select Permissions.
- 4 Review permissions so that only the system and administrators have Full Access. Review Special Access rights so that write access is only permitted to administrator or system users.

To remove DCOM RunAs from the registry:

- 1 [Open the Registry Editor.](#)
- 2 Go to the HKEY_LOCAL_MACHINE\Software\Classes\AppID key.
- 3 Locate the subkey(s) that use the RunAs value. Remove this value to restore the DCOM user context to that of the calling user. The scanreg utility from the Windows NT Resource Kit is also useful in locating these values.

To secure DCOM from the Interactive user:

- 1 [Open the Registry Editor.](#)
- 2 Go to the HKEY_LOCAL_MACHINE\Software\Classes\AppID key.
- 3 From the Security menu, select Permissions.
- 4 Double click the Interactive user.
- 5 Disable all write permissions for the Interactive user and click OK.
- 6 Enable 'Replace Permission on Existing Subkeys.'
- 7 Click OK.

To disable IP Forwarding in Windows NT:

- 1 [Open the Network control panel.](#)
- 2 Click Protocols.
- 3 Select TCP/IP Protocol from the list of network protocols.
- 4 Click Properties.
- 5 Select Routing.
- 6 Disable IP Forwarding.
- 7 Click OK twice to apply changes.

If you want to disable this function remotely, open the registry on the remote host and locate the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters key. Set the IPEnableRouter value to zero. You will need to reboot the remote host to apply this change.

To remove the POSIX or OS/2 subsystem from Windows NT:

- 1 Open the Registry Editor
- 2 Go to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems key.
- 3 Locate the Posix or Os2 value.
- 4 Write down the file name that is referenced by the value's data.
- 5 Remove the value.

To remove the files associated with the POSIX or OS/2 subsystem:

- 1 Open Windows NT Explorer or My Computer.
- 2 2 Using the path and file name you noted in step 4 above, remove the file that used to be referenced by the registry.

To disable the Network Monitor agent:

- 1 [Open the Services control panel.](#)
- 2 Select the Network Monitor service and click Stop.
- 3 To permanently disable the service, click Startup, click Disabled, and click OK.
- 4 Click Close.
- 5 Delete BHSUPP.DLL from %systemroot%\system32.

To run a Windows NT service under specific user rights:

- 1 As Administrator, create or modify a user account with the permissions required to run the service.
- 2 [Open the Services control panel.](#)
- 3 Select the service.
- 4 Click Startup.
- 5 Click '...' to the right of This Account field. The Add User window appears.
- 6 Select the user that will be used to run the service and click OK.
- 7 Type and verify the password.
- 8 Click OK.
- 9 [Restart the service.](#) or changes are applied during the next startup.

To enable the screen saver password:

- 1 Open the Display control panel.
- 2 Click the Screen Saver tab.
- 3 Enable Password Protected.

To require the screen saver password for all users:

- 1 [Open the Registry Editor.](#)
- 2 Go to the HKEY_USERS\.Default\ControlPanel\Desktop key.
- 3 Set the ScreenSaveActive value to 1
- 4 Set the ScreenSaverIsSecure value to 1.

To remove a Windows NT service:

- 1 [Open the Services control panel.](#)
- 2 Locate and record the exact spelling for the service name.
- 3 [Stop the service.](#)
- 4 Click Close.
- 5 From a Windows NT command prompt, type `instsrv service-name remove`.

To remove Administrator access from a user account:

- 1 [Open the User Manager.](#)
- 2 Double click the Administrators group, or the group you use to assign administrative rights.
- 3 Remove any unexpected Members. Look for the following:
 - User accounts or groups that do not need administrative rights.
 - User accounts or groups that are disabled or obsolete.
- 4 The Guest account should *not* be a member of Administrators unless there is a compelling reason.

To set user rights:

- 1 [Open the User Manager.](#)
- 2 From the Policies menu, select User Rights. The User Rights Policy dialog appears.
- 3 In the Right field, select the right you want to view or modify.
- 4 The Grant To field displays the names that currently possess this user right. Select one of the following options:
 - To grant user rights, click Add and [select the users or groups.](#) Click OK.
 - To revoke user rights, select the name from the Grant To list and click remove.
- 5 Click OK.

To set advanced user rights:

- 1 [Open the User Manager.](#)
- 2 From the Policies menu, select User Rights. The User Rights Policy dialog appears.
- 3 Click Show Advanced User Rights.
- 4 In the Right field, select the right you want to view or modify.
- 5 The Grant To field displays the names that currently possess this user right. Select one of the following options:
 - To grant user rights, click Add and [select the users or groups.](#) Click OK.
 - To revoke user rights, select the name from the Grant To list and click remove.
- 6 Click OK.

To add users or groups:

- 1 From the Add Users and Groups dialog, select the appropriate computer or domain from the List Names From field.
- 2 Select one or more users or groups from the Names list.
- 3 Click Add. The selected names appear in the Add Names list.

To set Security Settings in Internet Explorer 4.x:

- 1 Open Internet Explorer 4.x.
- 2 From the View menu, select Internet Options.
- 3 Click the Security tab.
- 4 Select the appropriate Zone.
- 5 Click Custom (for expert users).
- 6 Click Settings.
- 7 Locate the security feature and set it to the recommended value.
- 8 Click OK twice to apply the changes.

File Menu

The following commands are available from the File menu:

Command	Description
Scan Now	Starts a scan.
Stops Scan	Stops a scan that is running.
Pause Scan	Pauses a scan that is running.
Resume Scan	Resumes a scan that is paused.
Hide Console	Closes the console and leaves the agent running in the background. In this mode, the agent will run any scheduled scans. Click on the tray icon to show the console.
Close and Exit	Closes the user interface and stops the agent. In this mode, System Security Scanner will not run scheduled scans. To access the console, System Security Scanner must be restarted.

View Menu

The following commands are available from the View menu:

Command	Description
Toolbar	Shows or hides the toolbar.
Status Bar	Shows or hides the status bar.

Policy Menu

The following commands are available from the Policy menu:

Command	Description
New	Creates a new policy.
Delete	Deletes a policy
Rename	Renames a policy
Edit	Edits an existing policy
Copy and Edit	Creates new policies based on existing ones
Reset Baselines	Resets baselines for selected policies

Settings Menu

The following commands are available from the Settings menu:

Command	Description
General	<ul style="list-style-type: none">• Runs a scan at a low priority in the background• Runs a scan at system startup• Purges the scan results database• Secures the installation directory
Schedule	Schedules a scan to run based on a schedule you define.

Report Menu

The following commands are available from the Report menu:

Command	Description
Vulnerabilities	View and export vulnerabilities reports
Services	View and export services reports
Trends	View and export trends reports
Differential	View and export differential reports

Help Menu

The following commands are available from the Help menu:

Command	Description
Contents and Index	Displays the online help system
Product Updates	Installs micro updates
About System Scanner	Displays program information, version number, and copyright information

{ewl RoboEx32.dll, WinHelp2000, }

