Global Information Assurance Certification Paper

Microsoft Windows NT 4.0
Security Configuration Requirements
for High-Risk Workstations

GIAC Certification
Windows NT Security
Practical Application Requirement

SANS Network Security 2000
Monterey, California

Jerry Bollig

Table of Contents

This page is intentionally blank.

1 DOCUMENT FORMAT

1.1 Plan Format

The overall goal of this plan is to ensure that security features for workstations using Microsoft Windows NT 4.0 are correctly implemented.

All existing workstations using the Microsoft NT Operating System at This Company must be configured according to this document. All new high-risk NT workstations will be configured using the current document version.

This security configuration requirement contains a summary statement of a security Feature. For each Feature description there is a configuration or set of configurations that support or verify that the feature has been correctly implemented.

Each test description consists of five parts.

1. The first component, Test, is an assertion about a security attribute of the system or a statement describing the item to be tested.
2. The second component, Method, is a general statement that describes the method that is used to verify the assertion.
3. The third component, Expectations, describes the test results that must be observed. The results can be analytical (data), screen capture (show what should be seen), or theoretical (results derived from calculated or empirical information).
4. The fourth component, Results is the test result. Possible outcomes are:
   a. PASSED or FAILED (with tester initials and date of testing). FAILED indicates that the feature was tested, but fell short of the criteria specified in the expectation or the expectation is not correct for the configuration being tested. A FAILED test can be explained in the Comments section and may not invalidate the configuration.
   b. NOT TESTED. The test does not apply to the configuration being tested or circumstances prevent testing. In either case the test comments must indicate why the test was not conducted.
5. The fifth component, Comments, is used to describe any additional information such as unique test procedures, resources needed to run the test, explain test results, etc.).

1.2 Document Organization

This manual is organized into chapters. Each chapter includes configuration information for high-risk computers. All chapters must be performed.

1.3 Documentation Required for High-risk Accreditation:

Fill out this Configuration Requirements document for each computer configured unless multiple computers are configured identically within the same time interval (one-week). If you configure multiple computers identically within the same time interval, submit a single copy of the appropriate chapter(s) and a list of all computers configured. Include the following information: date, who configured each computer,

S-number, IP address, MAC Address, and Location.

1.4 Passwords:
There are multiple passwords generated during the configuration and delivery of a computer.

a. User's "Boot" (BIOS) Password.
b. System Administrator's "Boot" (BIOS) Password for the Local computer.
c. User's Network logon Password (used to log onto the network).

Follow the Policies stated below when configuring computers:

System Administrator's Password for the local computer's BIOS (computer setup). System administrators that administer multiple workstations/servers may have a common SA "Boot" (BIOS) Password. SA passwords must be randomly generated, passwords. This password may not be an SCN Kerberos password.

User's "Boot" (BIOS) Password. The local user selects this Password. It may not be the users network logon password, or any subset of the logon password.

System Administrator's Network Password for the Local computer. System administrators that administer multiple workstations/servers may have a common SA NT Logon Password. The System Administrator must obtain an Entity account from Password Control. The Entity account establishes a userid and password for the SA. SA must not use their SCN personal userid and password to administer client workstations.

User's Network logon Password (used to log onto the network): Password Control issues this password. The user must have this password before the computer is configured.

1.5 Workstation Update Policy
Non-critical updates to the Workstation Configuration Requirements document are released every four months. Non-critical updates do not require immediate installation. The installer may elect to install these updates to accommodate normal maintenance schedules. All workstations must be fully updated yearly and the NTMD SA notified of the date that the computer is fully compliant with current updates.

Critical updates are released as required to maintain the security configuration of the workstation and must be installed on all High-risk NT computers within 30 working days of receipt.

2 OBJECTIVE

The following configurations are considered a minimum set of configurations to ensure that NT 4.0 systems provide basic security protections. The tests are designed to validate that a Windows NT 4.0 operating system implementation meets expectation. The Microsoft Windows NT Administrator's Guide, Version 4.0, may be used in conjunction with the following tests to identify additional parameters and permissions that need to be set..

Microsoft also provides a C2 Configuration Management Utility that can automate the implementation/testing of some of the security features identified in the following tests. **DO NOT** execute, or use, the Microsoft C2 Configuration Management Utility, as it configures some items that do not necessarily need to be configured and does not configure some items required by this document.

3 PHYSICAL ACCESS

This section covers physical security controls required for workstations located in Vaults, Vault Type Rooms (VTR) and unprotected physical environments.

3.1 This section covers physical security protections for workstations located in a Vault or a VTR with Non Common Need-to-Know information access.

Feature:	High-risk workstations are located in a Vault-Type Room.

3.1.1 Workstations located in a VTR.

Test: Verify that the workstations are located in a VTR.

Method:
1. Locate each workstation.
2. Review the VTR certification letter.

Expectation: The VTR is an accredited room and all servers and/or workstations are located within the VTR.

Results: Passed ___ Failed ___ Not Tested ____ Initials _____ Date _____

Comments:

Feature:	If unclassified workstations are located in the Vault Type Room, the media in the high-risk workstations must be incompatible with any media in the unclassified computer (workstation or server).

3.1.2 Incompatible Media

Test: Verify that high-risk workstation media is incompatible with media in any unclassified computer in the vault.

Method: Inspect the high-risk workstations and unclassified workstations and/or servers.

Expectation: The media in the high-risk workstation(s) is incompatible with media installed in any unclassified computer in the vault. The media incompatibility is visually observable (e.g. locks, different types of media). Software enforced incompatibility does not meet the intent of this requirement.

Results: Passed ___ Failed ___ Not Tested ____Initials _____ Date

_____

Comments:

3.2 This section covers physical security protections for workstations located *outside* a vault or VTR.

Feature:	High-risk workstations not located in a Vault-Type Room (VTR) must use removable media.

3.2.1 Workstations not in a VTR

Test: Verify that high-risk computer not located in a VTR has removable media (e.g. hard-drives, JAZ, Bernoulli cartridges, etc.).

Method: Inspect the Workstations.

Expectation: High-risk Workstations not located in the VTR have removable hard drives.

Results: Passed ___ Failed ___ Not Tested ____Initials _____ Date _____

Comments:

Feature:	High-risk workstations located in a workspace with unclassified workstations or servers must have incompatible media.

3.2.2 Incompatible Media Requirements

Test: Verify that high-risk workstation media is incompatible with media in any unclassified computer in the workspace.

Method: Inspect the high-risk workstations and unclassified workstations and/or servers.

Expectation: The media in the high-risk workstation(s) is incompatible with media installed in any unclassified computer in the workspace. The media incompatibility is visually observable (e.g. locks, different types of media). Software enforced incompatibility does not meet the intent of this requirement.

Results: Passed ___ Failed ___ Not Tested ____Initials _____ Date

_____

Comments:

4 WORKSTATION CONFIGURATION

Feature: An administrator setup password (also called "power-on", "boot" or "CMOS" password) is used to configure the computer and to access the computer with privileges. The system administrator controls computer setup password length and age. The password(s) must be protected as SRD. The power-on password and the NT-logon password *may not* be the same. Multiple workstations may have the same administrator power-on password. The password(s) must be sealed in an envelope, marked SRD. and maintained in the department's high-risk repository.

Workstations need both a user power-on password, and an administrator power-on password unless they are located inside a VTR.

4.1 Power on passwords

4.1.1 Access the workstation setup function

Test: Verify that an administrator's power-on password is required to access the hardware setup function.

Method: Shutdown the system (turn power off to the CPU). Turn power on and observe power on sequence. Attempt to access the hardware setup with a user's password, and again with the administrator's password.

Expectations: The administrator must be able to access the computer hardware setup functions.

Note: If the workstation used does not support an administrator power-on password, mark this section **Failed** and identify the computer type (mfg., model, and CPU)

Results: Passed ___ Failed ___ Not Tested ____ Initials _____ Date _____

Comments:

4.1.2 Administrator's power-on password protection.

Test: Verify that administrator's power-on password is protected as SRD.

Method: Review the password storage process. Check to ensure passwords are stored in an approved high-risk repository (SRD) and that the processes are uniformly used and understood.

Expectations: The power-on passwords are controlled at the SRD level and all administrators understand the requirements.

Results: Passed ___Failed ___ Not Tested ____Initials _____ Date _____

Comments:

4.1.3 Changing the Administrator's Password

Administrator's password changed on schedule.

Test: Verify that the administrator's power-on password is changed every six months.

Method: Interview the System Administrator. Review the power-on password process.

Expectations: The power-on password is changed every six months.

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

4.1.4 Changing the User's Password

User's power-on password is changed every 6 months. A user's password is not required if the workstation(s) are located in a VTR, therefore mark test 4.1.4 and 4.1.5 as "Not Tested" and indicate in the "Comments" section that the workstation is located in a VTR.

Test: Verify that the user's power-on password is changed every twelve months.

Method: Interview the System Administrator. Review the power-on password process.

Expectations: The power-on password is changed every 12 months.

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Feature: The user's power-on password does not have administrative privileges.

4.1.5 Check user's power-on password privileges

Test: Verify that user's power-on password has no administrative privileges.

Method: Power on the system and attempt to change the BIOS settings using the user's power-on password.

Expectations: The users power-on password cannot be used to change the computer's BIOS settings.

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Feature: The computer cannot be started, or reset, from the network.

4.1.6 Starting the workstation from the network

Test: Verify that the computer cannot be started from the network.

Method: From the computer's BIOS setup table, check that "Start from Network is disabled.

Expectations: The computer cannot be started from the network. If the computer does not support this feature, mark the test failed and list the computer manufacturer, make, and model in the comments section.

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Feature:	On High-risk workstations not located in a vault or vault-type room (VTR), the 3-½ inch floppy disk drive and CD-ROM must be configured so that they cannot be used to boot the system.

4.2 Workstations not in a VTR are non-bootable using the floppy drive.

Test: Verify that the 3-½ floppy drive cannot be used to boot the computer.

Method: Insert a pre-formatted 3-½ inch bootable floppy disk into the floppy drive. Power down, and then power up the system.

Expectations: The high-risk computer cannot be booted using a floppy disk.

Results: Passed ___ Failed ___ Not Tested ____ Initials _____ Date _____

Comments:

4.3 Disable CD-ROM boot capability.

Test: Verify that the CD-ROM cannot be used to boot the computer.

Method: Insert a bootable CD into the CD-ROM. Power down, and then power up the system.

Expectations: The high-risk computer cannot be booted using the CD-ROM.

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Note

Reboot/power up the computer and log onto the **Local Domain** as the **Administrator** before proceeding.

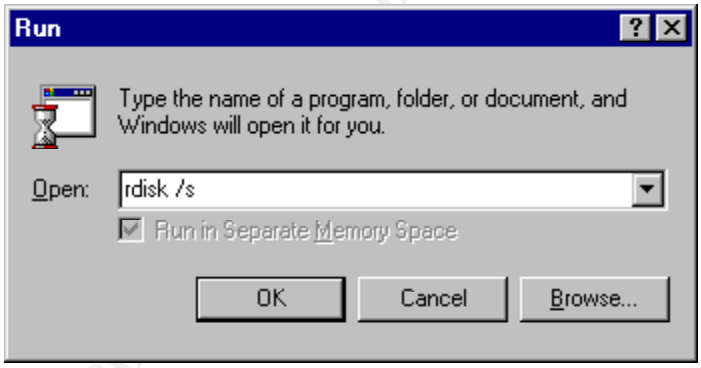
Feature: An Emergency Repair Disk (ERD) must be created before the configuration settings in this chapter are performed. The registry will be modified during the configuration process. Another ERD is created at the end of this document.

Note: The ERD contains a copy of the registry information and must be protected as High-risk and stored accordingly. Apply external label: "Protect as High-risk".

4.4 Creating an Emergency Repair Disk.

Test: Verify that the Emergency Repair Disk has been created.

Method: From Start | Run enter "**rdisk /s**" and hit **Enter**. Follow the prompts.



Example Illustration

Expectation: The Emergency Repair Disk has been created.

Results: Passed ____ Failed ___ Not Tested ___ Initials _____ Date _____

Comments: The Emergency Repair Disk must be marked and dated. It must be stored where only system administrators can get to it. If it is used after the High-risk computer has been connected to the SCN, it must be marked "Protect as High-risk" and stored at as High-risk material.

Feature: System is loaded with proper version of Windows NT with Service Packs**.**

4.5 Windows NT 4.0 and SP6a

Test: Verify installation of Windows NT 4.0 with Service Pack 6a.

Method: From the **START** menu select **Programs** | **Administrative Tools** | **Windows NT Diagnostics**, Select the **Version** tab. Read the text to ensure the appropriate version and Service Pack are installed.. Ensure that workstations do not have NT Server installed.

Expectations: The version of Windows NT and the Service Pack loaded must be displayed. The service pack displayed must agree with the appropriate service pack for the OS version as released by Computer Security.

Results: Passed ____ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Feature: If SP6a is installed **Post SP6** Hot-fixes must be loaded before releasing the workstation to the end user. Hot-fixes must be loaded in the sequence in the following table. Record all Hot-fixes installed in the table below.

NOTE: SP6a must be loaded for new installations

4.6 Post SP6a Hot Fixes Installation.

Test: Verify that SP6a Hot-fixes are installed and recorded.

Method: Connect to the SCNCAPP Server (\\Company-isn\sahp1287). Migrate to: | Source | NT40 | Service Pack 6a and Fixes | hotfixes_Post6a folder. Download and install the hot-fixes in the order in the table below. Record the hot-fixes installed. **Don't replace more recent DLL's.**

Expectation: Hot-fixes listed as of the date of configuration are installed and recorded.

	Hot Fix Name	PSS Id Number	Date
1.	C2Fix	Q244599i	
2.	Spooler-fix	Q243649	
3.	Winlogon-fix	Q245148i	
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Feature:	Directory and file level security is only available on drives that are NTFS configured. All **High-risk** storage media (except 3.5" floppy disks), including Bernoulli, JAZ, ZIP, or any type of storage media must be configured as NTFS.

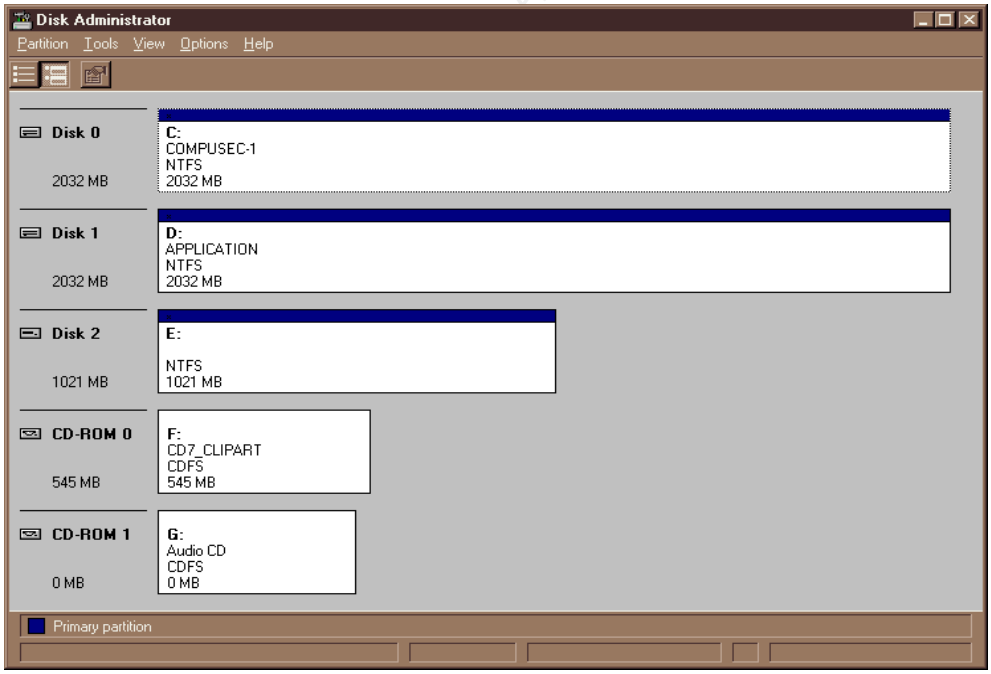
4.7 Configure all drives as NTFS.

Test: Verify that all drive partitions are formatted as NTFS.

Method: From **START** select **Programs** | **Administrative Tools** | **Disk Administrator**. Review the disk partition types. All writable storage media must be configured as NTFS. Eg. Type **convert *drive_letter*: /FS:NTFS /v**

*** Note ***

When a drive with a removable media (JAZ, Bernoulli, etc.) is converted from FAT to NTFS format, the ability to remove the cartridge during the windows session is eliminated. The cartridge can be removed only during power-down and initial boot when using the eject button on the Jaz drive. The cartridge can be ejected during operation by clicking on My Computer, then right click on Removable Disks, then click on Eject.



Example Illustration

Expectations: All writeable storage devices are configured as NTFS. JAZ and Bernoulli cartridges used with a High-risk system are marked to indicate they are configured as NTFS cartridges.

Results: Passed ___ Failed ___ Not Tested ___Initials _____ Date _____

Comments:

Feature: The system must be set up with the correct IP, DNS, and WINS addresses.

4.8 Set up the IP, DNS, and WINS addresses.

Test: Verify that the correct addresses have been inserted into the Network settings.

Method: Click on Start, Settings, Control Panel, Network, Protocols, TCP/IP Protocol, Properties. Click on the tabs, and verify the fields are set as follows:

a) Microsoft TCP/IP Properties IP Address tab

IP Address	NWIS IP Address of this computer
Subnet Mask	255.255.255.0
Default Gateway	192.218.22.254

Enter the Default Gateway of your local system.

Do not perform steps b) and c) if this is an autonomous domain (e.g. a local domain that has a PDC and is not a Resource domain).

b) Microsoft TCP/IP Properties window DNS tab

DNS Host Name	NWIS name of the machine
DNS Domain	Company.gov
DNS Service Search Order	192.218.19.5
	192.218.19.4

c) Microsoft TCP/IP Properties window WINS Address tab

Primary WINS Server	192.218.22.25
Secondary WINS Server	192.218.22.22

Expectations: The settings are as listed.

Results: Passed ___ Failed ___ Not Tested ___Initials _____ Date _____

Comments:

Feature:	Floppy disks and CD-drives are allocated at logon by settings of the registry hive.

4.9 Register settings for Floppy disks and CD drives.

Test: To ensure that only the user currently logged on can access floppy disks and CDs, verify that floppy disks and CD-ROM drives are allocated at logon.

Method: Using the Registry Editor, verify that the parameters "AllocateFloppies" and "AllocateCDRoms" values for Winlogon are set to 1.

If the values are not present, follow the following procedure:

1. Logon to the computer as administrator
2. Run the registry editor (regedt32)
3. Activate the **HKEY_LOCAL_MACHINE** subtree window
4. Go to the **SOFTWARE** key under **\Microsoft\WindowsNT\CurrentVersion\Winlogon subkey**,
5. Click on **Edit**;
6. Click on Add Value; Enter **AllocateFloppies** or **AllocateCDRoms** into the **Value Name** field; Enter **Data Type** of **REG_SZ**, and click on **OK**.
7. Enter **1** into the **String** field; Click on **OK.**
   A logical value "**1**" activates the feature.

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\Windows NT\Current Version\Winlogon
Name:	AllocateFloppies
Type	REG_SZ
String:	1
Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\Windows NT\Current Version\Winlogon
Name:	AllocateCDRoms
Type	REG_SZ
String:	1

Expectations: The Values must be set to one. If the Value is set to any other value, then floppy devices will be available for shared use by all processes on the system or other users on the system or network. (Sharing of CDs may be operationally acceptable, particularly if software is shared via the CDs. Otherwise, need-to-know will be the determinant. Mark this section ***Failed*** and Contact Computer Security for configuration instructions if CDs need to be shared.)

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Feature:	Automatic restoration of the Registry with .reg files should not be possible except by the administrator.

4.10 Remove association of regedit with .reg files.

Test: Configure the Registry so that .reg files don't update the Registry.

Method: Using the Registry Editor (regedt32), set text associated with the following registry key value, changing **regedt.exe** to **notepad.exe**:

Hive:	HKEY_LOCAL_MACHINE\Software
Key:	\Classes\regfile\shell\open
Name:	command
	Highlight the data field, then double-click. In the String Editor window, change *regedit* to *notepad.*
String:	Notepad.exe "%1"

Expectations: The registry is set as indicated.

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Feature:	The Windows NT Pagefile can contain sensitive information, and should be cleared upon shutdown.

4.11 Clear the Pagefile at Shutdown.

Test: Configure the registry so that the Pagefile is cleared upon shutdown.

Method: Using the Registry Editor (regedt32), set text associated with the following registry key value as follows:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	\CurrentControlSet\Control\Session Manager\Memory Management
Name:	ClearPageFileAtShutdown
Type	REG_DWORD
String:	1

Expectations: The registry is set as indicated.

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date

_____

Comments:

Feature: OS/2 and POSIX are disabled.

4.12 Disable OS/2 & POSIX

Test: Verify that OS/2 and POSIX subsystems are disabled.

Method: Using the Registry Editor (regedt32), click on each of the following named values, then click on delete to remove the values.

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Control\Session Manager\SubSystems
Name:	**Optional**
Name:	**OS/2**
Name:	**Posix**

Expectations: The Value fields must be removed. This means that OS/2 and POSIX will not be loaded at system boot up. Installation of an operating system other than NT would compromise system security.

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Feature: Access to the scheduling service must be limited to administrators.

4.13 Set access to the Scheduling Service.

Test: Verify that access to scheduling the service is limited to administrators.

Method: Using the Registry Editor (regedt32), verify the text "SubmitControl" is not present. Remove it if it is present.

Expectations: The file permissions must be as:

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Control\Lsa
Name:	SubmitControl (remove if present)

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Feature:	Permanent account lockouts due to login failures should not allow access to the user list from a null session.

4.14 Enable RestrictAnonymous.

Test: Verify that an intruder could not engage in password guessing attacks and lock out all users in that domain or host.

Method: Using the Registry Editor (regedt32), add the value **RestrictAnonymous** if it is not present. Click on **EDIT**, then **Add Value**.

Expectations: The file permissions must be as:

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Control\Lsa
Name:	RestrictAnonymous
Type	REG_DWORD
Value	1

Results: Passed ____Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Feature:	LanManger (LM) challenge/response authentication should not be allowed.

4.15 Eliminate LanManager challenge/response authentication.

Test: Configure the Register to eliminate LanManager authentication.

Method: Using the Registry Editor (regedt32), add the following value . Click on **EDIT**, then **Add Value**.

Expectations: The file permissions must be as follows:

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Control\Lsa

Microsoft Windows NT 4.0 Configuration Requirements

Name:	LMCompatibilityLevel
Type	REG_DWORD
Value	2

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Feature:	By default, the Logon Information dialog box includes a Shut Down button that can be used to shut down the workstation without having to log on first. The Shut Down button must be removed from the Logon Information dialog box to prevent a user from shutting down the workstation without first logging on and being validated as an authorized user of the computer.

4.16 Disable the ShutDown button.

Test: Verify system shutdown is limited to logged-on users.

Method: Boot\reboot, the computer and observe the Logon Information dialog box. Using the Registry Editor (regedt32), verify text associated with the following registry key value is as follows:

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\Windows NT\Current Version\Winlogon
Name:	ShutdownWithoutLogon
String:	0

Expectations: In the Logon Information dialog box, the Shut Down button must be grayed out indicating it is not active.

Notes: A procedure to disable the Shut Down button is:

1. Logon to the computer as administrator
2. Run the registry editor
3. Activate the **HKEY_LOCAL_MACHINE** subtree window
4. In the **SOFTWARE** key under **\Microsoft\WindowsNT\CurrentVersion\Winlogon subkey, observe the ShutdownWithoutLogon:REG-SZ** value entry. A logical value "**1**" enables the Shut Down button, a "**0**" disables the Shut Down button. Set the value to "**0**".

Results: Passed ___ Failed ___ Not Tested ____Initials _____ Date _____

Comments:

Feature:	User notification of LAN policies is required at logon for High-risk systems.

4.17 Logon Legal Notice.

Test: Verify that a logon legal notice is displayed.

Method:
1. Shut down the system. Power the system up. Observe the logon legal notice, or
2. Use the Registry Editor (**Start|Run|regedt32**) to observe/edit the banner text.

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\Windows NT\Current Version\Winlogon
Name:	LegalNoticeCaption
Type	REG_SZ
String:	"**Login Security Notice**"

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\Windows NT\Current Version\Winlogon
Name:	LegalNoticeText
Type	REG_SZ
String:	"Company computers are for Official Use Only. (Etc.)"

Expectations: The display of a logon legal notice must include, *but is not limited to*, notification to a user that this is a Company National Laboratories network, it is monitored, it must only be used for official purposes, misuse can result in disciplinary action. The format of a *minimal* legal notice is:

Format

"Company computers are for Official Use Only. Users are responsible for protecting information and passwords they control; avoiding waste, fraud, or abuse of computing resources; using only authorized software; and obeying SNL/DOE security policies. Users have no implicit or explicit expectation of privacy. Use of SNL computers is subject to monitoring and review by authorized SNL personnel. Improper use may result in disciplinary or legal action. "

Note: One procedure to install a login notice is:

1. Login to the local machine as Administrator.
2. Run the Registry Editor. From run, type **regedt32** <cr>
3. Activate the **HKEY_LOCAL_MACHINE** subtree window
4. View the **\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon** subkey.

NOTE: This part sets the text displayed in the banner.

5. Observe the **LegalNoticeCaption** and the **LegalNoticeText** value entries. They must be blank and of data type **REG_SZ**.
6. Double-click on the **LegalNoticeCaption** key
7. Enter the string value such as **WARNING!** Or whatever you want your users to see upon bootup, Click on **OK**

NOTE: This part sets the text displayed in the warning box.

8. Double-click on the **LegalNoticeText** key. Enter a string value
9. Exit the registry editor.
10. Reboot the system and check the Warning Message.

The LegalNoticeCaption appears in the Banner of the pop-up box, while the LegalNoticeText will appear within the box.

Results: Passed ____ Failed ____ Not Tested ___ Initials _____ Date _____

Comments:

Feature:	The Microsoft NT registry controls the ability to boot the workstation and how the workstation boots. Only administrators are able to change the registry, by any means.

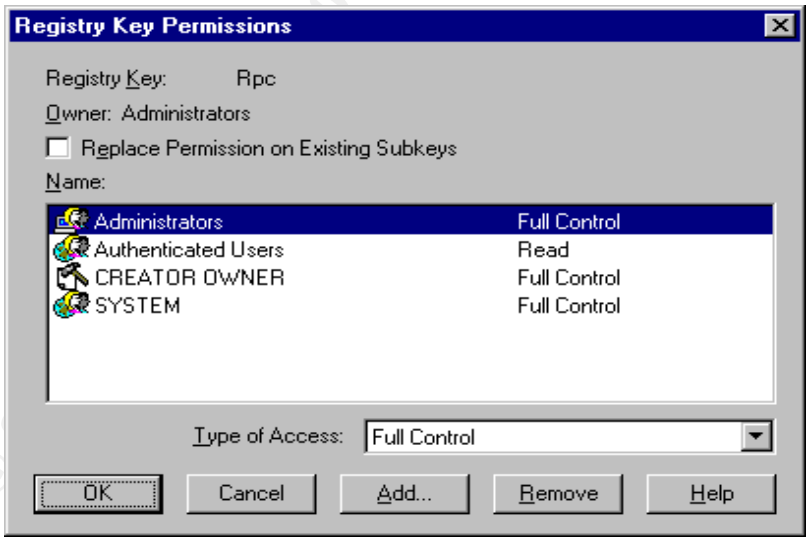
4.18 Verify the Registry Keys Protection.

Test: Verify Registry keys are protected.

Method: Using the Registry Editor (**regedt32**), and from the toolbar **Security | Permissions**, verify the registry values of the keys in the following table.

Registry Key: (RPC and Keys from the following table)	
Administrators	Full Control
Authenticated Users	Read
CREATOR OWNER	Full Control
SYSTEM	Full Control

Expectations: The following keys, and subtrees must be set so that the group "Authenticated Users" is only allowed **READ** (QueryValue, Enumerate Subkeys, Notify, and Read Control) accesses for the registry keys shown in the table. Users should be added or removed as required so that only the following users and permissions are allowed. The group *Authenticated Users* is added from the *USER Domain*, if required.



Example Illustration

Hive:	**HKEY_LOCAL_MACHINE\SOFTWARE**
Key:	\Microsoft\RPC (and its subkeys)
Key:	\Microsoft\WindowsNT\CurrentVersion\
Subtrees:	AeDebug
	Compatibility
	Drivers
	Embedding
	Fonts
	FontSubstitutes
	GRE_Initialize
	MCI
	MCI Extensions
	Midimap
	Ports
	Profile List (and all subkeys)
	WOW (and all subkeys)
Hive:	**HKEY_LOCAL_MACHINE\SOFTWARE**
	Windows3.1MigrationStatus (and all subkeys)
Hive	**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows**
	CurrentVersion (and all subkeys)
Hive	**HKEY_LOCAL_MACHINE\SOFTWARE**
Subtrees	Classes\regfile\shell\open\
Key	command
Hive	**HKEY_LOCAL_MACHINE\SYSTEM**
Subkeys	CurrentControlSet\Control\SecurePipeServers
Key	Winreg (and all subkeys) Include only Administrators and System
Hive:	**HKEY_CLASSES_ROOT** (and all subkeys)

Mandatory Registry Settings

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Note: Close the Registry after this step.

Feature: OS/2 and POSIX directories are removed.

4.19 Remove OS/2 and POSIX directories.

Test: Verify that OS/2 and POSIX directories are removed.

Method: Right click on Start, and select Explore. In the Explorer toolbar, select View -| Options, then check "Show all files", and make sure "Hide file extensions of known files" is NOT checked. Save this setting.
Remove the following files in the **%system root%\system32** directory.
1. os2.exe
2. os2srv.exe
3. os2ss.exe
4. posix.exe
5. psxdll.dll
6. psxss.exe

Remove the directory C:\%SYSTEM ROOT%\SYSTEM32\OS2
Empty the Recycle Bin.

Expectations: Inspect the **%system root%\system32 directory**. The files listed above must not be present.

Results: Passed ___ Failed ___ Not Tested ____ Initials _____ Date _____

Comments:

Feature:	Proper operation and protection of Windows NT requires that critical directories and files are protected at the directory and file level. The file system must be NTFS to continue.

4.20 Operation System files and directories protections.

Test: To ensure that the operating system files and directories are appropriately protected.

Method: From the File Manager (Explorer), select the root drive (e.g. C:, D:, etc.) and set the permissions, as appropriate, on each drive as indicated in the table below:

NOTE:
Ensure the "Replace Permissions on Subdirectories" box is not checked and the "Replace Permissions on Existing Files" box is checked in the Directory Permissions popup window.

Directory	Permissions
Drive (root)	Administrators: Full Control SYSTEM: Full Control Owners SCN userid (USER***userid***)*: Full Control
All user directories (on all drives)	USER***userid****: Full Control SYSTEM: Full Control CREATOR OWNER: Full Control
\%SYSTEM ROOT%\REPAIR	Administrators: Full Control SYSTEM: Full Control
\%SYSTEM ROOT%\SYSTEM32/-NTBACKUP.EXE	Administrators: Full Control SYSTEM: Full Control
\%SYSTEM ROOT %\SYSTEM32\DHCP	Administrators: Full Control SYSTEM: Full Control
\%SYSTEM ROOT %\SYSTEM32\RAS	Administrators: Full Control SYSTEM: Full Control
\%SYSTEM ROOT %\SYSTEM32\WINS	Administrators: Full Control SYSTEM: Full Control

Expectations: The directory and file permissions are set properly.
The warning about the "Pagefile is in use" is OK".

Results: Passed ___ Failed ___ Not Tested ____ Initials _____ Date _____

Comments:

Feature:	Some files are critical to the boot, operation, and recovery of an NT system. These files must not be observable, or alterable by users except authorized system administrators.

4.21 Protection of critical operating system files.

Test: On Intel and Pentium-based systems: Verify that several critical operating system files exist in the root directory of the system partition and are properly protected.

Method: From the File Manager (Explorer), review the permissions of the files below.
If the files are not visible, then click on View, Folder Options, and View, then select *Show all files*. Reset to *Do not show hidden or system files* after setting the permissions.

Expectations: The file permissions must be as below:

File	Permissions
\BOOT.INI, \NTDETECT.COM, \NTLDR \AUTOEXEC.BAT, \CONFIG.SYS	Administrators: Full Control SYSTEM: Full Control

Example Table

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

NOTE:

Remove all *.bak files at this level

Feature: All computers and users are registered in Company's NWIS database. NWIS issues a unique computer name to the computer when it is registered. NWIS issues a unique user name to each Company staff member. The Company NWIS database maintains the user and computer name.

4.22 NWIS Computer Name Verification

Test: Verify that the computer name matches the NWIS-registered computer name.

Method: Select START; Settings, Control Panel, and select the Network Icon. Check that the Computer Name listed matches the registered name for the computer.

Expectations: The computer name must match the NWIS-registered computer name.

Example Illustration

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

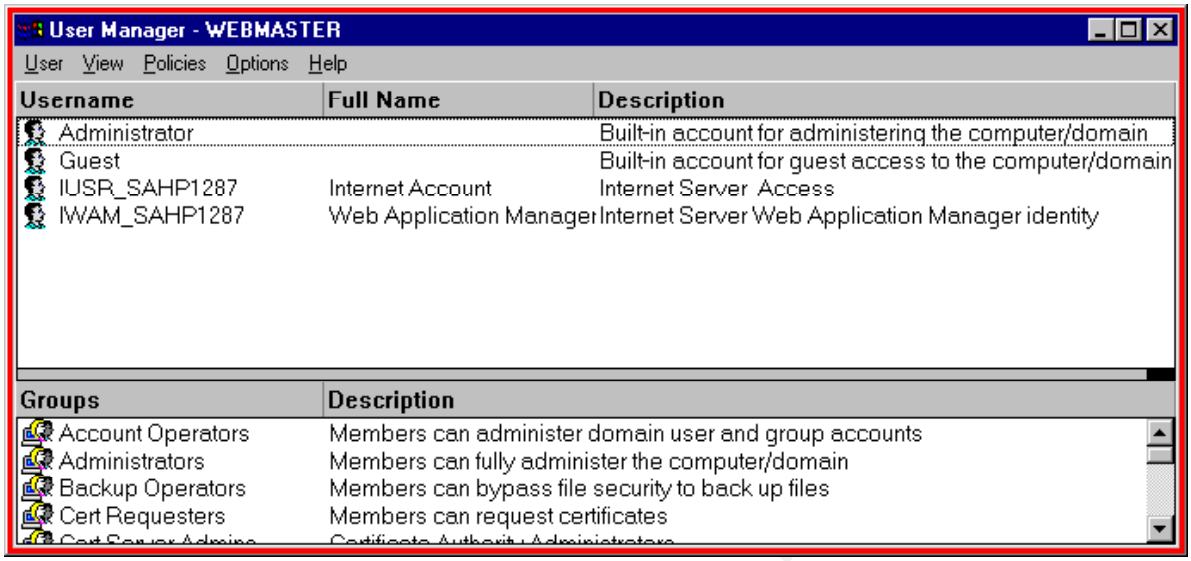
Feature: Local users have access to all local files on their computer after being validated by the PDC. The only account that can be used to log onto the workstation, at the workstation, is the local administrator's account. No users accounts are maintained on the workstation.

4.23 Check local user accounts.

Test: Verify that there are no local user accounts on the workstation. Local accounts for SMS, IIS, or other third-party software may be on the workstation.

Method: Select **START| Programs | Administrative Tools (Common),** and select **User Manager**. Check that the account names listed in the User name column match the registered administrator names for the users.

Expectations: The only accounts on the workstation are the default accounts shown. Local accounts for SMS, IIS, or third-party software is acceptable.



Example Illustration

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Feature: Users on a network must have no user-privileges other than those needed to perform their assigned tasks.

t the User Rights and Policies

Test: Verify user rights are restricted to the minimum required.

Method: From the User Manager window, evaluate the system wide rights policy by comparing each right with those as shown in the table below.

Note: "----------" means No Access.

Process	Permissions
Access this computer from network	Administrators USER***userid**
Act as part of the operating system	----------
Add workstations to domain	----------
Back up files and directories	Administrators Backup Operators
Bypass traverse checking	----------
Change the system time	Administrators USER***userid**
Create a pagefile	----------
Create a token object	----------
Create permanent shared objects	----------
Debug programs	----------
Force shutdown from a remote system	Administrators
Generate security audits	Administrators
Increase quotas	----------
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	----------
Log on as a batch job	----------
Log on as a service	----------
Log on locally	USER***userid** Administrators
Manage auditing and security log	Administrators
Modify firmware environment values	----------
Profile single process	----------
Profile system performance	Administrators
Replace a process level token	----------
Restore files and directories	Administrators Backup Operators
Shut down the system	Administrators Backup Operators USER***userid**
Take ownership of files or other objects	Administrators

Expectations: User rights must be as indicated in the referenced table. For

example: Unless required by operational necessity, "Debug Programs" is to be removed from all accounts, including Administrators, as it is not auditable.

Results: Passed ___ Failed ___ Not Tested____Initials _____ Date _____

Comments:

Feature: Disable the User's ability to Change their password.

4.25 Disable the Change Password function

There are no user accounts authorized on this workstation. Therefore the user of the workstation does not have a local user's account that could be changed.

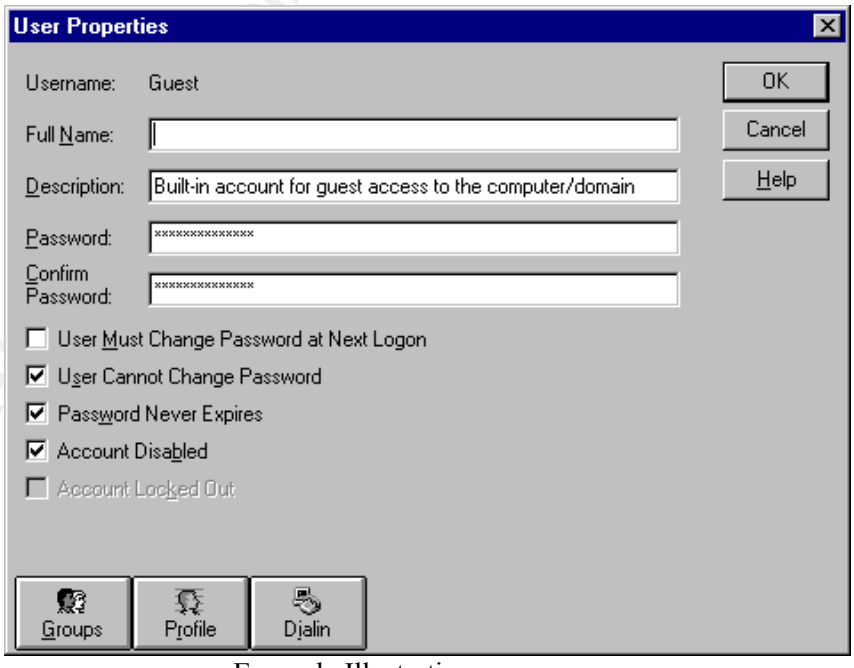
Feature: Disable the Guest account to prevent unauthorized access to a workstation.

4.26 Disable the Guest account.

Test: Verify that the "Guest" account has been disabled.

Method: From the User Manager window, double click on "Guest."

Expectations: The "Account Disabled" box must be checked.



Example Illustration

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

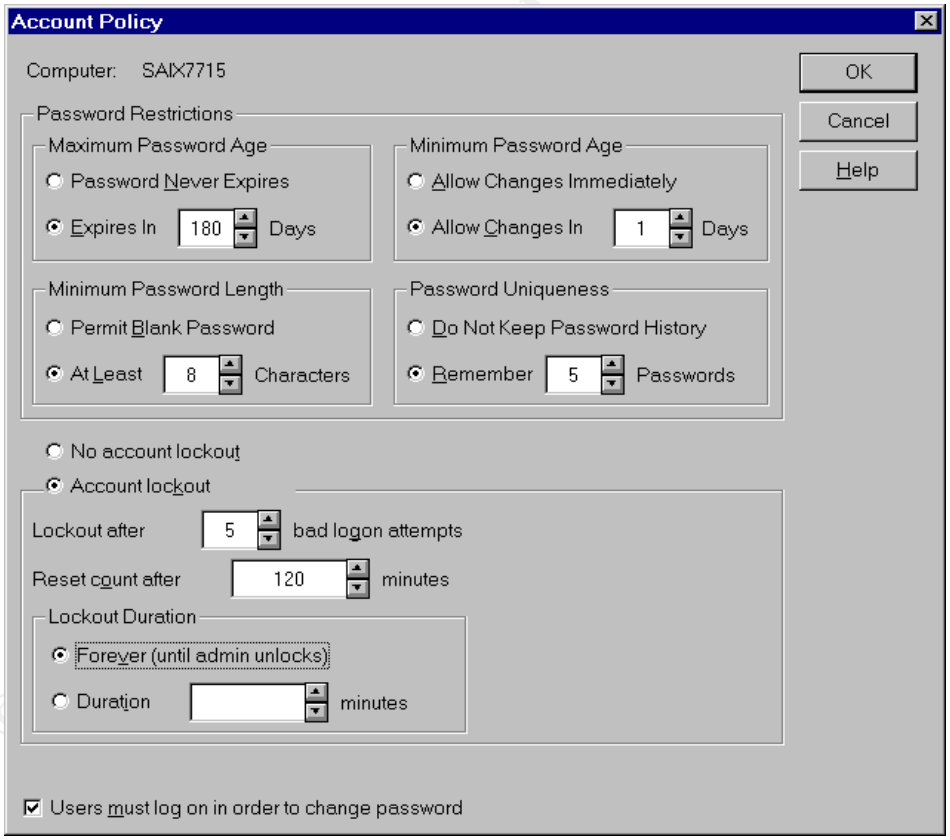
Feature:	Password age and length are controlled, the number of unsuccessful log on attempts is counted and an account lockout is established after a predetermined number of unsuccessful logon attempts.

4.27 Password age and length

Test: For High-risk Workstations verify the following parameters:

Method: From **Start | Program | Administrative Tools, | User Manager**, select **Policies/Account**.

1. maximum password age is **180** days
2. minimum Password age: **Allow Changes in 1 Days**
3. minimum password length is **At Least 8 Characters**
4. Password Uniqueness **Remember 5 Passwords**
5. **Account lockout** is selected
6. **Lockout after 5 bad logon attempts** is selected
7. **Reset count after 120 minutes** is set
8. **Lockout Duration** is set for **Forever(until admin unlocks)**
9. **Users must log on in order to change password** is checked



Example Illustration

Expectations: The parameters are set as indicated in the Illustration.

Results: Passed ____ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

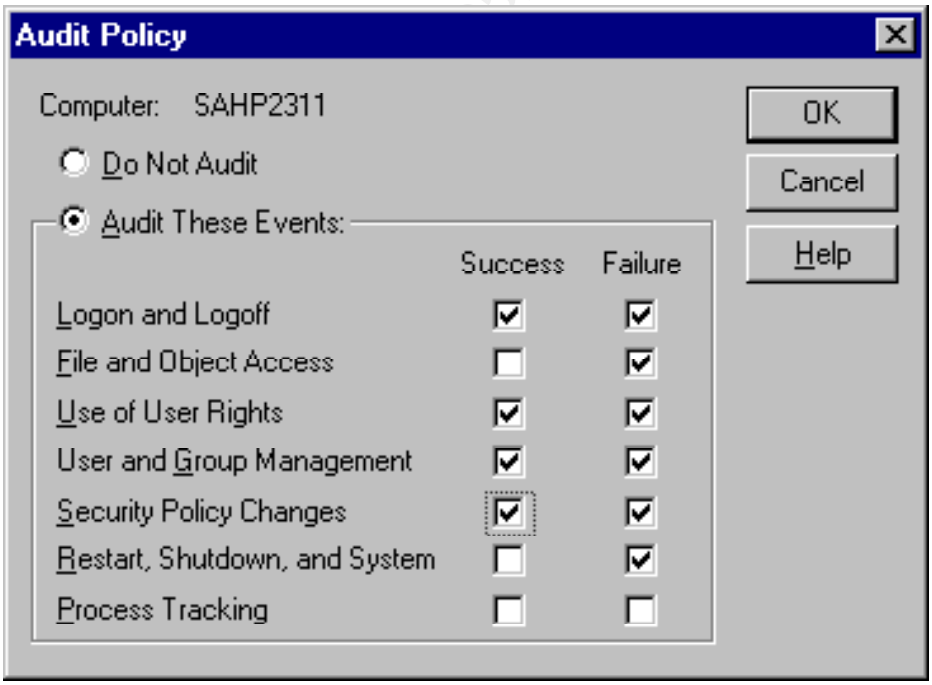
Feature:	Auditing of users attempts to login, successful and unsuccessful, and failure to access data or applications must be automatically tracked.

4.28 Auditing of users' logon attempts and data access failures.

Test: Verify that auditing is set up to record all successful and unsuccessful login attempts to the node and all attempts to access data or resources that result in denial of access, and all network service attempts (i.e., connections).

Method: From User Manager/Policies, review the Audit Policy parameters.

Expectations: At a minimum, "Logon and Logoff", "File and Object Access," "Use of User Rights," "User and Group and Management," "Security Policy Changes", and "Restart, Shutdown, and System" must be checked under the Failure column. "Logon and Logoff", User and Group Management", "Security Policy Changes" and "Restart, Shutdown, and System" options must be checked under the Success column.



Example Illustration

Results: Passed ___ Failed ___ Not Tested ___Initials _____ Date _____

Comments:

Feature:	The security log records user events on the network. These records provide an audit trail of user and account activity. There are three logs 1) System, 2) Security, and 3) Application. All three logs need to be set according to the configuration shown below.

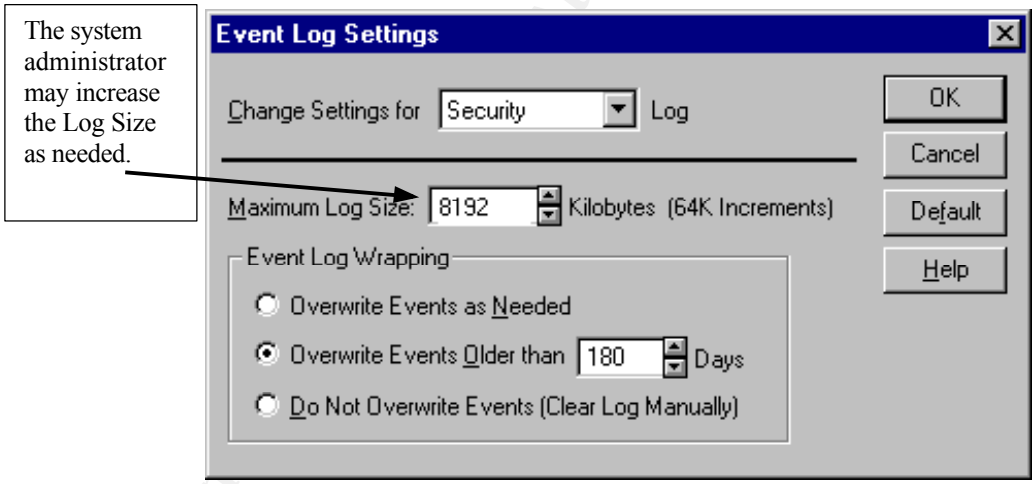
4.29 Event Log Settings

Test: Verify the event log settings are:

a) Maximum Log Size is at least 8192 Kilobytes.
b) Event Log Wrapping is set to "Overwrite Events Older than 180 days"

Method: From **START** | **Programs** | **Administrative Tools (Common)** |**Event Viewer**. Select the pull-down menu **Log → Log Settings**. Change Settings for each of the three logs (System, Security, Application)

Expectations: The System, Security and Application logs are correctly set.



Example Illustration

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Feature:	Access and ability to change audit logs form the basis of all audits. Only authorized administrators with proper authorization can have access to these files. General users cannot have any access to the audit files.

4.30 Control access to audit logs

Test: Verify that the "read/write" access to files containing audit information is restricted to those with proper authorization (e.g., administration or audit-privileged accounts).

Method: From the Explorer or by using My Computer and the folders, review the Security Permissions of the audit files with an extension of **.evt** in **\%system root%\system32\config**. Hardcopy logs must be locked away from general user access.

Expectations: The SYSTEM and ADMINISTRATOR have full control.

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Feature:	The Alerter and Messenger Services can be a source of vulnerability and must be disabled.

4.31 Disable the Alerter and Messenger Services.

Test: Verify that the Alerter and Messenger Services are disabled.

Method: From **Start -| Settings**, select **Control Panel**. Select the **Services**. From the Services popup select Alerter then select Startup. In the **Service** popup select the **Disabled** radio button. Click **OK**. Select the **Messenger** service, then select **Startup**. In the **Service** popup select the Disabled radio button. Click **OK** then **close**.

Expectation: The Alerter and Messenger Services are disabled.

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

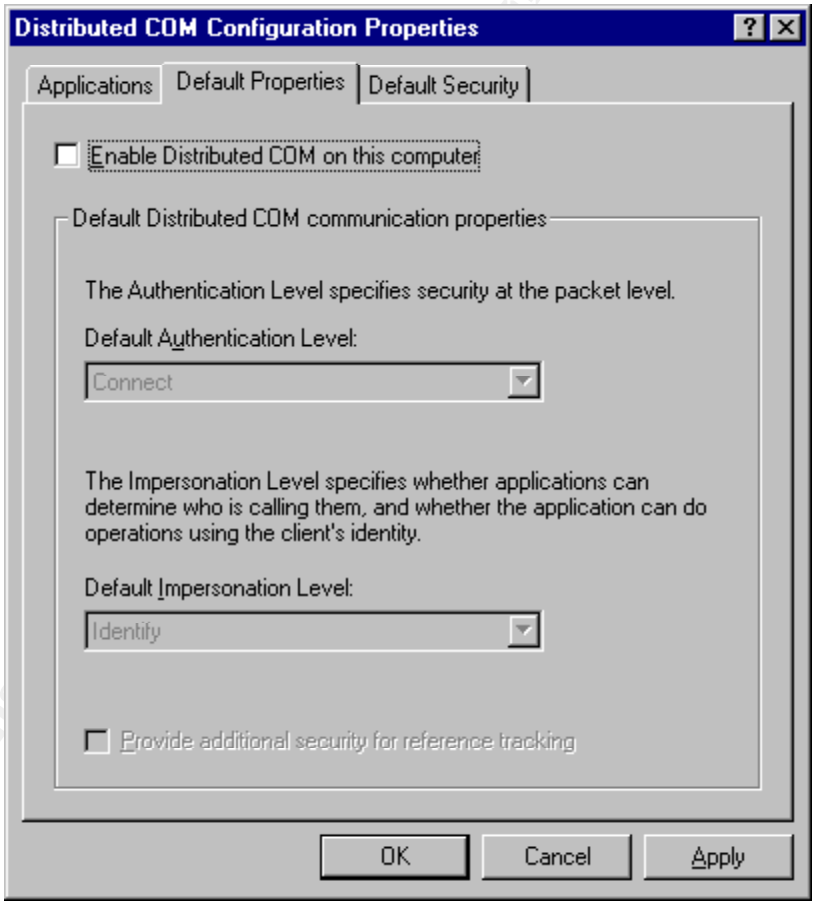
Comments:

Feature:	The DCOM Distributed Computing Facility in NT 4.0 is currently the source of a major security vulnerability. This facility must be disabled on High-risk systems.

4.32 Disable DCOM.

Test: Verify that the DCOM Distributed Computing Facility is disabled.

Method: From "**Start**" select"Run" and enter "**dcomcnfg**" in the select box. Select the"**Default Properties**" tab and assure that the checkbox labeled "**Enable Distributed COM on this Computer**" is **NOT** checked.



Example Illustration

Expectations: The "Enable Distributed COM on this Computer" is not enabled.

Results: Passed ___ Failed ___ Not Tested ___Initials _____ Date _____

Comments:

Feature: Rename the Administrators account to prevent attacks at local site.

4.33 Rename the Administrators account.

Test: Verify administrators account information.

1. The Administrators account has been renamed. The renamed account must follow NWIS naming conventions (e.g. mswoaa).
2. Change the description so that it does not indicate that this is an administrator's account.
3. The renamed administrator's account and password must be written down, sealed in an envelope, marked as SRD, and stored in the department's High-risk repository.

Method: From the "User Manager" window, click on the renamed Administrator account (e.g. mswoaa). Select Group and check that the user is a member of the administrators group.

Expectations: The administrator account is named in accordance with NWIS guidelines.

Results: Passed ___ Failed ___ Not Tested ___Initials _____ Date _____

Comments:

Feature: Create a "decoy" account for Administrator.

Note: The decoy administrator account password must be an 8-character, alphanumeric password. It must be written down and stored as High-risk.

4.34 Create a "decoy" account for Administrator.

Test: Verify administrators account information.
A new account called Administrator has been created.
This account belongs to no groups.

Method: From the "User Manager" window, select New User.
Type Administrator in the Username window.
Check the Account Disabled check box.
Give the account an 8 character, alphanumeric password.

Expectations: The administrator account has no group membership.

Results: Passed __ Failed __ Not Tested __ Initials _____ Date _____

Comments:

Feature:	Screen savers ***are not*** used to protect High-risk information. High-risk workstations must be attended during high-risk processing by staff member(s) that have common NTK for the information being processed. The information displayed on the monitor must be automatically protected after a period of no keyboard activity. Installed NT Screen Savers must be used and password protected. The inactivity time is be set for 15 minutes (max) (The inactivity time can be set to less than 15 minutes).

4.35 Screen Saver

Test: Verify that the workstation invokes an NT Screen Saver after **at most** 15 minutes of keyboard inactivity and is password protected.

Method: Monitor the system and check to ensure an NT Screen Saver appears after a max of 15 minutes of keyboard inactivity and that the Screen Saver is password protected.

Expectations: If a screen saver is used, a password protected NT Screen Saver that activates within 15 minutes is used.

Results: Passed __ Failed __ Not Tested __ Initials ____ Date _____

Comments:

Feature:	An Emergency Repair Disk (ERD) must be created or updated when service packs or major applications are added. The ERD can be created or updated after installation of Windows NT 4.0 by using the rdisk /s command from the Command Prompt Window. This ERD captures the changes made to the registry during the configuration. Do not use the ERD created in 8.4.
NOTE:	The ERD contains a copy of the registry information and must be protected as High-risk and stored accordingly. Apply external label: "Protect as High-risk".

4.36 Emergency Repair Disk.

Test: Create or Update the Emergency Repair Disk.

Method: From **Start** | **Run** "command". Then enter "**rdisk /s**".

Expectation: The Emergency Repair Disk now reflects the installed system configuration.

Results: Passed ___ Failed ___ Not Tested ___ Initials _____ Date _____

Comments:

Reboot the computer before continuing.

Caution Caution Caution Caution

Microsoft NT 4.0 sets all directories and files with "**Everyone**" having **Full Control**. Data directories must be created for only the users or groups which need access and

1. The group **Everyone** must be removed
2. Security Permissions must be set so that the data-owner, or the owner of the computer has **Full Control**. The administrator may or may-not be granted access to the directories. Access is determined by the data owner, not the administrator
3. The installer must ensure that the data owner understands how the Security Permissions are set, why they must be set, what must be set, and how to check the permissions on directories and files

If questions arise concerning directory policies and/or permissions, contact the local NT Administrator or the Computer Security Department.

Caution Caution Caution Caution

2 References

Fossen, Jason and Kolde, Jennifer. (2000) Securing Windows NT, Step by Step, Parts 1-3: Monterey, Ca: The SANS Institute

Schultz, Eugene (2000) Windows NT/2000 Network Security: Macmillan Publishing

Schultz, Eugene (1999) Windows NT Security, Advanced, Parts 1 & 2: San Francisco, Ca: The SANS Institute