GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at http://www.giac.org/registration/gcwn

Windows NT Web Server Auditing

By Dean Farrington

© SANS Institute 2000 - 2002, Author retains full rights.

Written for Sans GCNT Certification Practical
10/22/2000

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Introduction:

This document is to outline procedures for auditing the Windows NT 4.0 operating system for use as a production web server. I have written this document to be used in two ways, first as a resource to draw steps to secure a webserver from, and then once the steps have been determined you can remove the extra commentary and use this document as a checklist both for the securing process and then the auditing process.

The document is intended to show best practices, and then additional steps that can be applied to achieve full bastion hosting of the server. Many of these steps that implement the extra security of Bastion Hosting will break certain integral functionality of the OS. I will endeavor to document the things that will be affected by each step as a risk so that this document can be used as the basis for web server security plans. As always test all security hardening steps on a non-production web server prior to deployment.

The steps contained here are drawn from numerous sources, best practices guides, and the experience of running IIs 4.0 in a production web farm environment. Most of the steps in this document are presently in use on bastion-hosted servers in a corporate DMZ.

Assumptions:

This checklist is written under the assumption that you are placing your production web server into a DMZ using bastion-hosting practices to ensure optimal security. I am also presuming that the servers will be standalone servers acting as webservers. Creating a webserver on a domain member adds some complication to the hardening process as you have to allow some normal domain traffic that is not required on a stand alone server.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

NT Web Server Auditing Checklist

Project #_____ Date Audit Performed:_____

Server:_____ Audit Performed By: _____

General Section:

☐ **Computer installed as a standalone server**

Reason: Proper domain functionality requires communications channels that are Not appropriate for use within a DMZ. If IIS is installed on a Domain Controller the IUSR_*MachineName* is placed in the Domain Users group. This will provide the IUSR account access to all computing platforms participating in the domain.

☐ **Ensure there are 2 Drive Partitions (one for OS, and 1 for Applications/data) both formatted with NTFS.**

Reasons: Best security can be achieved by segregating Web Content from Operating system files. NTFS file systems allows permissions to be assigned down to the level of the individual file making it the best choice from a security standpoint.

☐ **Current SP and all necessary hotfixes installed**.
Reason: It is important to always use the most up to date Microsoft Service packs And relevant hot fixes. They contain fixes for known problems in the OS and Web Server. Check the Security Bulletins at Http://www.microsoft.com/security for the latest security risks and links to current patches. While you are there I recommend you subscribe to the e-mail alert newsletter, that way you will get notices of the new warnings as they are released.

List Fixes Installed:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

☐ **Make certain there are no shares or printers configured**.
Reason: Shares provide an access point into a server, for best security none Should be allowed. Shares are dependant on the Server Service which we will Be disabling in a later step. Also a DMZ based server should not be printing. It is extra system overhead that should be unnecessary. If printing is determined to be required be sure to apply all relevant patches for the spooler service.

☐ **Only IIs installed as an application**
Reason: Any extra applications provide an avenue for security problems. A Bastion Host is a server that is hardened to provide only one service.

☐ **Disable all unneeded services**

NT Server provides a variety of services that are not needed on a bastion hosted web server. All unneeded services should be disabled both to improve performance and close potential back doors into the system.
Refer to the Microsoft Knowledge Base article Q189271 for further information

These are the minimum services that must be running:

- IIS Administration
- NT and LM Security Service Providers
- Protected Storage
- Remote Procedure Call Service
- Event Log Service
- World Wide Web Publishing service

Document any other services running and the reasons for leaving them enabled

☐ **Disable the binding for the Wins client from network interfaces**

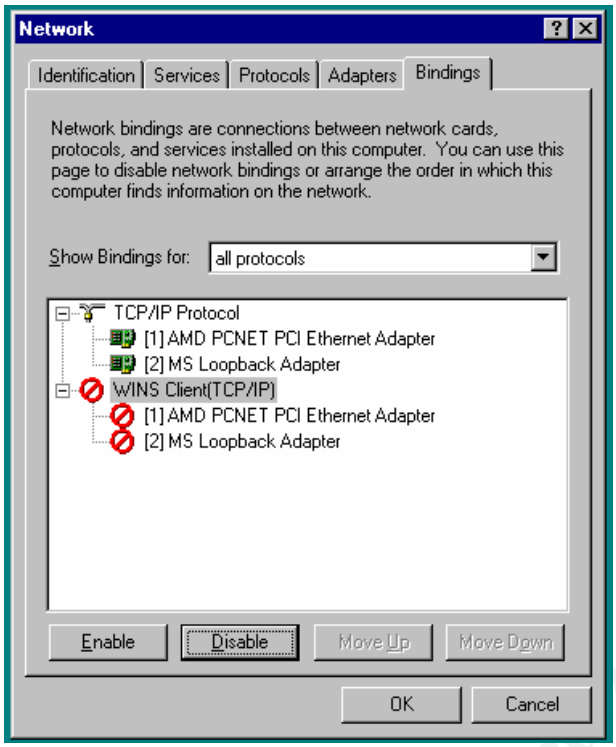
Open **<CONTROL PANEL> <NETWORK> <BINDINGS>.**

In the **SHOW BINDINGS FOR** drop down menu select **<PROTOCOLS>.**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Highlight the **WINS CLIENT (TCP/IP)** field and click **<DISABLE>.**

Reboot the server.



Reason: this will fully block port 139 which is a preferred method of entry by hackers. If you are multihoming your server be sure the Network Interface facing the external firewall has the Wins client disabled.

Risk: Once this is disabled File sharing, and NetBIOS name resolution will no longer function.

☐ **Use Syskey to encrypt the Sam database**

Reason: Passwords on NT servers can be cracked using a variety of hacker tools. Syskey is a utility installed with Service Pack 3 or later, it can provide additional encryption on the SAM database. You install the encryption by running the Syskey command in a dos prompt. You are presented with a dialog box used to activate the encryption

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

followed by one asking where the key for the encryption should be stored. Your options are stored locally on the hard drive, stored on a floppy disk, or provided as a password at system boot.

Risk: Using either the floppy disk storage or boot time password can be risky in a high availability environment. In either case something must be provided at boot time or the boot process will hang.

Important Note: If Syskey is used be sure to also apply the patch for MS99-056 which fixes an issue with the key use.

Reference: See Microsoft Knowledge Base Article Q143475 for additional details.

☐ **Use the C2config utility from the resource kit to heighten security**:

1) Remove the O/S2 and Posix Subsystems

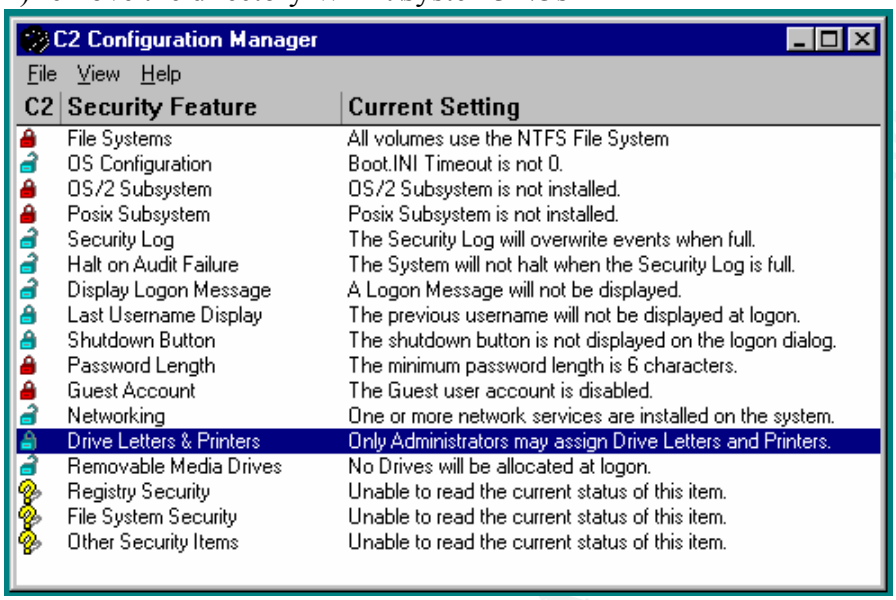
2) Set the don't display last logged on user name property
This adds the following registry key for you

Hive:	**HKEY_LOCAL_MACHINE**
Key:	**SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon**
Name:	**DontDisplayLastUserName**
Type	**REG_SZ**
Value:	**1**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3) Allow only Administrators to assign drive letters and printers

4) remove the directory Winnt\system32\Os2



Reason:

The OS/2 and Posix subsystems are for compatability with legacy systems. They should not be required on a production webserver and therefore removed to reduce risk.

The setting Last Username Display sets the registry value DontDisplayLastUserNAme for you. This prevents someone from seeing a locked server and learning what a valid account name is to attempt to brute force passwords against.

Allow only Administrators to assign drive letters and printers restricts settings users should not be accessing on a server.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

File and Registry Permissions:

☐ **Secure NTFS permissions**

Reason: Default NTFS file permissions on an NT server are extremely relaxed. Tightening permissions is necessary to ensure that unauthorized users do not have access to files that are inappropriate. NTFS also enables File Auditing.

Using the group Authenticated Users instead of the everyone group restricts the files that are accessible to Null Session connections. Do not apply these permissions to all subdirectories.

from the root of C:\ and D:\	set Administrator = Full Control System = Full Control Authenticated users = Read
\Winnt	set Administrator = Full Control System = Full Control Authenticated users = Read
\Winnt\System32	set Administrator = Full Control System = Full Control Authenticated users = Read
C:\Winnt\Repair	set Administrator = Full Control
C:\Winnt\System32\Config	set Administrator = Full Control System = Full Control Authenticated Users = List
C:\Temp	set Administrator = Full Control System = Full Control Authenticated Users = Special Read, Write, and Execute

Set permissions on these critical Operating System Files:

File	Permissions
\Boot.ini **\Ntdetect.com** **\Ntldr**	**Administrators: Full Control** **SYSTEM: Full Control**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

\Autoexec.bat **\Config.sys**	**Everyone: Read** **Administrator: Full Control** **SYSTEM: Full Control**

☐ **Change Registry Access Permissions as follows**:

Registry Key Access Rights

Apply the permissions listed below such as query value, enumerate subkeys, etc. to the **EVERYONE** Group only. **Do not** replicate to the subkeys unless instructed to do so. These permissions equate to **READ** only for the **EVERYONE** Group.

Access Granted for **EVERYONE** Group:
QUERYVALUE, ENUMERATE SUBKEYS, NOTIFY and **READ CONTROL**

HKEY_LOCAL_MACHINE Permission Sets

HKEY_LOCAL_MACHINE on Local Machine dialog:
\SOFTWARE Note: this change controls who can install software. It is **not recommended** that the entire subtree be locked with this setting since that can render certain software unusable.

\SOFTWARE\MICROSOFT\RPC (and **ALL** subkeys) This locks the RPC services.
\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\PROFILE LIST

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\AEDEBUG

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\COMPATIBILITY

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\DRIVERS

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\EMBEDDING

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\FONTS

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\FONTSUBSTITUTES

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\FONT DRIVERS

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\FONT MAPPER

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\FONT CACHE

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\GRE_INITIALIZE

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\MCI

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\MCI EXTENSIONS

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\PERFLIB

Remove **EVERYONE:READ** access to this key. This prevents remote users besides administrators and the System Account from seeing performance data on the computer. Instead you could give **INTERACTIVE:READ** access that will allow only interactively logged on user access to this key.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\PORT (and **ALL** subkeys)

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\TYPE1 INSTALLER

\SOFTWARE\MICROSOFT\WINDOWS NT\ CURRENTVERSION\WOW PORT (and **ALL** subkeys)

\SOFTWARE\ \WINDOWS3.1MIGRATIONSTATUS PORT (and **ALL** subkeys)

\SYSTEM\CURRENTCONTROLSET\SERVICES\LANMANWORKSTATION\SHARES

\SYSTEM\CURRENTCONTROLSET\SERVICES\UPS

In addition to setting security on this key, the command file (if any) associated with the UPS service must be appropriately secured, allowing **ADMINISTRATORS: FULL CONTROL**, **SYSTEM: FULL CONTROL** only.

\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN

\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUNONCE

\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL

1. **HKEY_CLASSES_ROOT** Permission Sets

HKEY_CLASSES_ROOT on Local Machine dialog:
\HKEY_CLASSES_ROOT (and **ALL** subkeys)

2. **HKEY_USERS** Permission Sets

HKEY_USERS on Local Machine dialog:
\.DEFAULT

3. Registry Subkeys

Registry Key	Permissions
Registry Key: **HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\ WINDOWS NT\CURRENTVERSION\WINLOGON**	**CREATOR OWNER: FULL CONTROL** **ADMINISTRATORS: FULL CONTROL** **SYSTEM: FULL CONTROL** **EVERYONE: READ**

☐ **SET NTFS permissions on the following Special Directories**
Requirement: These NTFS permission settings must be used for IIS content "virtual" directories.

File Type (Suffix)	Permission Granted
CGI (exe, .dll, .cmd, .pl)	**AUTHENTICATED USER GROUP**: **EXECUTE** only **ADMINISTRATORS** and **SYSTEM: FULL CONTROL**
SCRIPT (asp)	see above
INCLUDE (inc, shtml, .shtm)	see above

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

STATIC CONTENT (html .gif, .jpeg)	**AUTHENTICATED USER GROUP**: **SPECIAL READ**, (no Execute) **ADMINISTRATORS** and **SYSTEM: FULL CONTROL**

Registry Modifications:

☐ **Ensure that guests and null logons do not have the ability to view logs** (system, security and application logs).

Hive:	**HKEY_LOCAL_MACHINE**
Key:	**\System\CurrentControlSet\Services\EventLog\[LogName]**
Name:	**RestrictGuestAccess**
Type	**REG_DWORD**
Value:	**1**

Reason: Access to these logs should be restricted to authorized personnel.

☐ **Restrict Remote Registry Access**
HKEY_LOCAL_MACHINE\CurrentControlSet\Control\SecurePipeServer\
Add the key Winreg and set the permission to "Deny" for everyone

Reason: This prevents anyone from connecting to the system registry remotely. Remote registry access can allow commands to be added to the registry that will execute at boot or log on. It can allow a hacker to trick you into executing commands for them

☐ **Make certain that administrative shares have been disabled in the registry**

Hive:	**HKEY_LOCAL_MACHINE**
Key:	\System\CurrentControlSet\Services\ LanmanServer\ Parameters
Name:	**AutoShareServer**
Type	**REG_DWORD**
Value:	**0**

Reason: This disables the default administrative shares C$, D$, and Admin$ These shares can provide an inroads into a server and should be disabled.

Risk: Disabling the default administrative shares will break many of the commercial backup software packages. Be sure to test this prior to deployment in your environment

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Reference: Microsoft article Q245117

☐ **Use Passfilt.dll to ensure strong passwords**

Hive:	**HKEY_LOCAL_MACHINE**
Key:	**\System\CurrentControlSet\Control\Lsa**
Name:	**NotificationPackages**
Type	**REG_Multi_Sz**
Value:	**passfilt**

Add a REG_MULTI_SZ value called "Notification Packages" with a value of PASSFILT. If the value FPNWCLNT (File and Print Client for Netware) already exists, then remove it unless Netware interoperability is required

Reason: Passfilt.dll is used to require users to select strong passwords. It enforces the use of three of the four possible choices, Uppercase letters, Lowercase Letters, Numbers and Special characters in every password. Be aware however, passwords set by administrators are not subject to the same restrictions.

Reference: Microsoft article Q161990

☐ **Disable NTFS 8.3 character name generation**

Hive:	**HKEY_LOCAL_MACHINE**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Key:	**\System\CurrentControlSet\Control\Filesystem**
Name:	**NTFSDISABLE8DOT3NAMECREATION**
Type	**REG_DWORD**
Value:	**1**

Reason: An issue was discovered where the normal NTFS file permissions could be bypassed by using the 8.3 file name disabling.

Risk: Disabling this removes compatibility with some older applications.

Reference: Microsoft Q130694, Q121007, MS Internet Information Server 4.0 Security Checklist

☐ **Restrict Anonymous**

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

Reason: Restrict Anonymous prevents a non authenticated user from being able to Read registry values, and enumerate permissions and user accounts. If this value is not set a "Null Session" connection can enumerate all valid user accounts on a server.

Resources: Microsoft article Q143474, MS Internet Information Server 4.0 Security Checklist

☐ **Disable Logon Caching**

Hive:	**HKEY_LOCAL_MACHINE**
Key:	**\Software\Microsoft\Windows NT\CurrentVersion\winlogon**
Name:	**CachedLogonsCount**
Type	**REG_SZ**
Value:	**0**

Reason: Logon caching can allow a machine to logon a disabled or deleted user account if the network is not present. On a stand alone server this should never be

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

an issue as the Logon process is checking a local users database which should always be available, but this is a good sanity check setting.

☐ **Wipe the System Page File during clean system shutdown. This can be achieved by setting up the following key**:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	System\CurrentControlSet\Control\SessionManager\Memory Management
Name:	ClearPageFileAtShutdown
Type:	REG_DWORD
Value:	1

Reason: At system shutdown the contents of the PageFile can be written to the hard drive. Any information in memory at the time of the shutdown could potentially be found in the file pagefile.sys. This setting prevents unsecured data from being written to the hard drive.

Clearing the pagefile causes the information to be overwritten prior to system shutdown. This can cause the shutdown to take a few seconds longer.

Reference: Microsoft article Q182086

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

User Accounts:

☐ **Account Policy settings should be as follows:**

Option	Required Setting
Maximum age	60 days
Minimum age	1 day
Minimum length	6 characters
Uniqueness	6 passwords
Lockout option	3 bad logins
Reset option	1 hour
Lockout duration	Forever

☐ **Modify User Rights as follows:**

User Right	Groups assigned this right by default on stand-alone server	Change for stand-alone server
Log on locally. Allows a user to log on at the computer, from the computer's keyboard.	Administrators, Everyone, Guests, Power Users, and Users	Remove Everyone and Guests from having this right.
Shut down the system. (See Shutdown-Privilege) Allows a user to shut down Windows NT.	Administrators, Everyone, Guests, Power Users, and Users	Remove Everyone, Guests and Users from having this right.
Access this computer from the network. Allows a user to connect over the network to the computer.	Administrators, Everyone and Power Users	Administrators, Power Users and Users Add Authenticated Users

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

☐ **Modify the "Access this computer from the network" user right**.
Change it from Everyone to Authenticated Users.

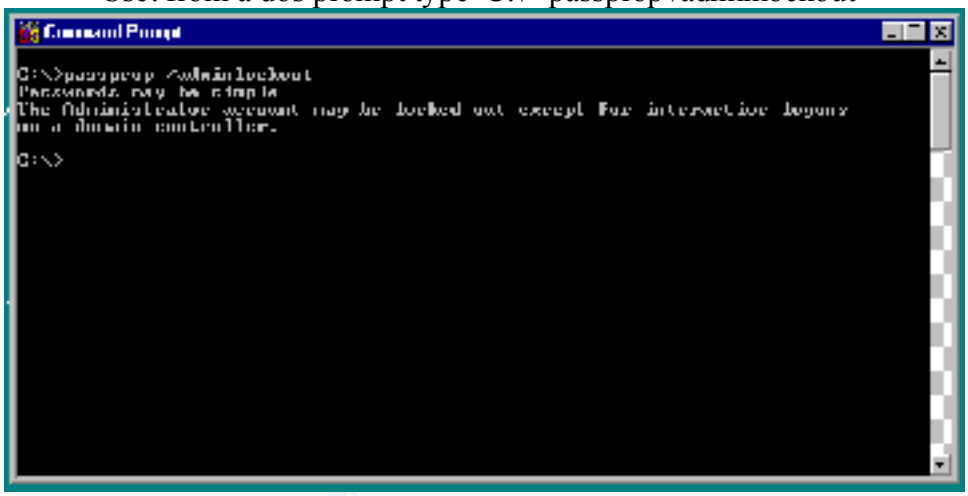
Reason: This is another measure to prevent "Null Sessions" from being able to Access the system

☐ **Use Passprop to allow Administrator lockout over the network**

Reason: The Administrator account cannot be locked out. Hackers know this, making it a prime point of attack for brute force password guessing.

The passprop utility available in the NT Resource Kit allows you to enable the Administrator account to be locked out for across the network connections. The Administrator account is always available interactively even if locked out with this utility.

Use: from a dos prompt type C:\> passprop /adminlockout



☐ **Rename the Administrator Account**.

Reason: Renaming the administrator account will not prevent someone from determining which account is the Administrator since the admin account is always RID 500, however it does add one more step that a hacker would have to go through.

Note: a new unprivileged account called Administrator can be created and heavily audited, for additional security.

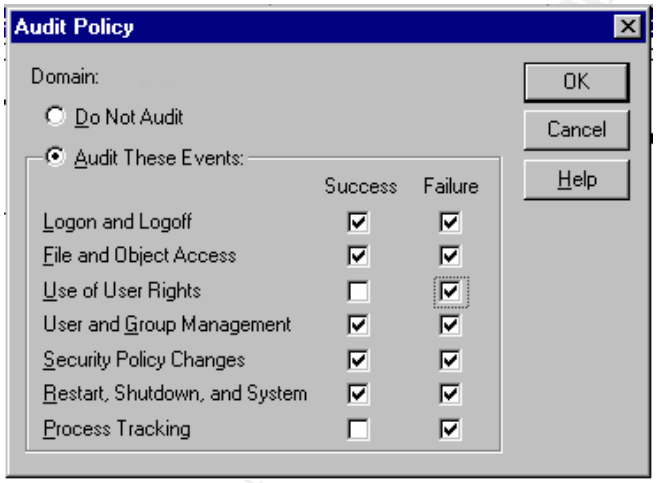
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Auditing:

☐ **Enable Auditing**

Reason: All Windows NT Servers should have Auditing enabled, requirements will vary with local policy but this is a recommendation. Auditing is enabled in the User Manager Under the policy pull-down menu.

Enable Auditing	Capture
Logon and Logoff	Success, Failure
File and Object Access	Success, Failure
Use of User Rights	Failure
User and Group Management	Success, Failure
Security Policy Changes	Success, Failure
Restart, Shutdown and System	Success, Failure
Process Tracking	Failure



Risk: The options "Use of User Rights" and "Process Tracking" are very intensive in terms of volume of logs generated. Activating both success and failure for both these items can add extra overhead to your servers operation.

Activate File and Object Auditing

Requirement: Activate file and object auditing for the **EVERYONE** Group as indicated below. Use the following audit parameters: select only **FAILURES - WRITE, DELETE, CHANGE** permission and **TAKE OWNERSHIP**. Apply to the following file/object types: (system root is assumed to be **C:**).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

C:\REPAIR

- **C:\WINNT** (do not replicate to subdirectories)
- **C:\WINNT\SYSTEM32** (do not replicate to subdirectories)
- **C:\WINNT\SYSTEM32\DRIVERS** (do not replicate to subdirectories)
- Application specific directories
- IIS related directories housing executable files like the **\SCRIPT** directory
- Closely monitor any attempt to access **.BAT** or **.CMD** files for possible exploit purposes

☐ **Audit the execution of Administrator Specific executables:**

Winnt\regedit.exe
Winnt\system32\regedt32.exe
Winnt\system32\telnet.exe
Winnt\system32\tft.exe
Winnt\system32\net.exe
Winnt\system32\net1.exe
Winnt\system32\rdisk.exe
Winnt\system32\Syskey.exe

These applications should only be used by the administrator, monitoring the success or failure of their execution will let you see who is attempting to make changes to your system. The net commands can be used to add users and modify the groups they are in, the tftp command can be used to get hacking tools onto a server, and rdisk (since it will update the users database) is frequently run by hackers to get the most current passwords to attempt to crack.

☐ **Registry Auditing Enabled**

Requirement: Activate file and object Auditing for the **AUTHENTICATED USERS** Group as shown below. Use these audit parameters: select only **FAILURES – SET VALUE, CREATE SUBKEY, DELETE**, and **WRITE DAC**. Apply to the Registry keys.

- **HKLM\SOFTWARE\MICROSOFT\<NET DRIVER>**
- **HKLM\SOFTWARE\MICROSOFT\LANMANSERVER**
- **HKLM\SOFTWARE\MICROSOFT\TCPIP**
- **HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION**
- **HKLM\SOFTWARE\CLASSES**
- **HKLM\SYSTEM\CCS\CONTROL**
- **HKLM\SYSTEM\CCS\SERVICES**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

IIS Specific Modifications:

☐ **Web content and WWWroots installed on secondary drive.**

Reason: using a secondary drive improves security by limiting your exposure to Parent Path exploits (where a malicious user can use the ../ notation to traverse the file system and see privileged files) and keeps your publicly accessible content away from system files.

Note: in a high traffic environment it is advisable to move your Traffic log files to the secondary drive as well. These tend to become very large and can be cumbersome to remove from the system drive.

☐ **IUSER_*MachineName* Not part of any privileged groups.**

Reason: The Iusr_Machinename account is used to map NTFS permissions To users accessing the web server anonymously. If the Iusr account is added to a privileged group anonymous internet browsers could potentially gain access to files they would not normally have access to.

☐ **IWAM_*MachineName* not part of any privileged groups**

Reason: The Iwam_Machinename account is used to run web based applications that are running out of process. If the Iwam account is added to a privileged group web based applications could be used to gain access to files or processes not normally accessible to the anonymous user. If you are not running applications out of process this account does not need the elevated privileges it possesses by default

☐ **Make sure the following physical directories are removed:**

IIS Samples
IIS Samples\SDK
AdminScripts
Program Files\Common Files\system\MSADC\Samples

Reason: There are numerous exploits for the IIs sample pages, and it is never a good practice to install samples on a production system. The Admin scripts directory allows extensive administration via Visual Basic Scripts. These should be taken off the system or moved and secured to prevent their exploit by anyone gaining access to the server.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

☐ **Remove the virtual directory /IIsampwd**

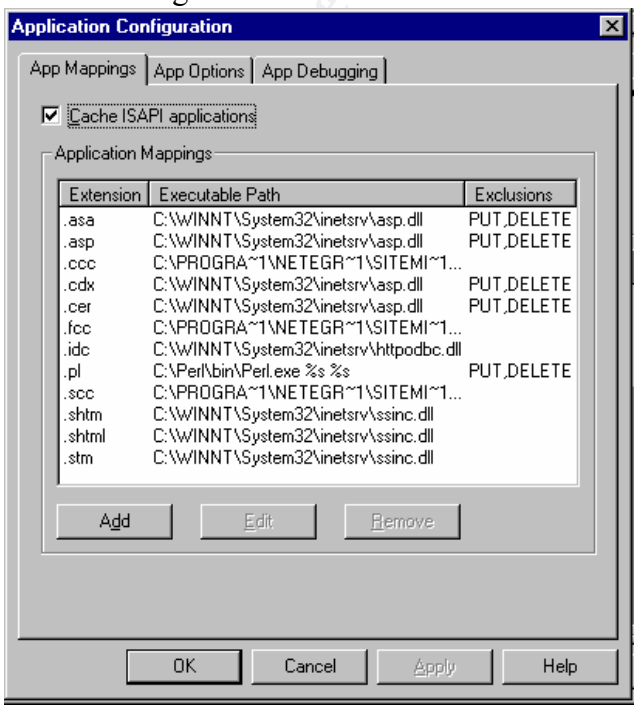
Reason: The Iisampwd is a sample application to allow passwords to be changed Via the internet. This page allows brute force attack against the system user accounts. As with the sample pages it should have no place on a production server.

Reference: Microsoft article Q184619

☐ **Remove Unused application mappings**:
.htr
.idc
.shtm
.stm
.shtml

Reason: The reasons for removing unused mappings are twofold, the first performance is slightly enhanced with fewer mappings and the second is security. As new exploits are discovered that affect the various application mappings, removing all not in use will help minimize the risk. There have been many issues discovered with the .htr application mapping, if it is not actively used it should be disabled.

In the MMC go to



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

☐ **Remove RDS functionality**

Reason: This is a serious security issue with the IIs web server addressed in Microsoft Security Bulletin MS98-004 (and re released as MS99-025). The Microsoft Data Access Components exposes some unsafe elements, which can be exploited to perform privileged actions. Unless this functionality is specificly needed it should be disabled. To fully disabled you must do both of these steps:

Delete the /msadc virtual directory from the default Web site

Remove the following registry keys from the server hosting IIS:

- 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

☐ **Do not index scripts directory**

Uncheck Index this directory on the IIS property sheet for the Virtual Directory

Reason: Scripts should not be browsed, indexing them will allow you to use the search engine to search for things that might be embedded in the script such as passwords,DSN information, or file paths.

☐ **Do not activate directory browsing**
Make sure the checkbox is cleared on the Site Property sheet

Reason: directory browsing allows the web server to return a list of all files in a directory when the page requested is not found. If it is activated a hacker can submit a url that requests a file that is not present and receive a listing of all files in the directory.

☐ **Remove Jet and text ODBC drivers if installed**.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Reason: There are exploits for both types of drivers.

☐ **Disable Parent Paths**

To disable this option, go to the root of the Web site in question, right click then **SELECT <PROPERTIES> <HOME DIRECTORY> <CONFIGURATION> <APP OPTIONS>** ad uncheck **ENABLE PARENT PATHS**

Reason: Parent Paths allow you to send the notation ../ to the webserver causing it To go back up one directory. This can allow someone to break out of the web root and access system files if they can determine the directory path. If it must be enabled be sure to keep the web contents on a secondary drive and use strong NTFS permissions

☐ **Disable Calling the command shell with #exec**.

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	\SYSTEM \CurrentControlSet \Services \W3SVC \Parameters
Name:	SSIEnableCmdDirective
Type:	REG_DWORD
Value:	0

Reason: Server Side Includes that call the command shell could be exploited to execute arbitrary commands with the privilege level of the webserver.

☐ **Document if sites are running in-process or Out of Process**

reason: This information could be important for troubleshooting in the future. Running a web site Out Of Process should allow a misbehaving application to not crash all of IIs, only that one website. It does mean that the application running out of process runs under the context of the IWAM account and this requires the Iwam account to be given higher level permissions.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

High Security Options:

These modifications enhance security further but can interfere with some functionality. Evaluate the benefits of each change before implementing it, and test its effects on a non-production server prior to placing on a production webserver

System Options:

☐ **Secure ODBC Tracing**

ODBC call tracing should be restricted to administrative users
. The following steps should be followed while logged in as an **ADMINISTRATOR**:

1. Log in to the machine you are protecting as the machine or domain administrator. Using **REGEDT32.EXE**, take ownership of the following key:

   HKEY_LOCAL_MACHINE
   SOFTWARE
   ODBC
   ODBC.INI

2. Set the value **TRACE** to **0**. The **TRACE** value can be found under the following Registry key:

   HKEY_LOCAL_MACHINE
   SOFTWARE
   ODBC
   ODBC.INI
   ODBC

3. Set the value **TRACEDLL** to an empty string. The **TRACEDLL** value can be found under the following Registry key:

   HKEY_LOCAL_MACHINE
   SOFTWARE
   ODBC
   ODBC.INI
   ODBC

4. Set the permissions for Authenticated Users to **READ** on the **ODBC** key.
5. Remove explicit permissions on the **ODBC** key for any non-administrative users.

For each user, there is a Registry file. This file is named **%SYSTEMROOT%\PROFILES\USERNAME\NTUSER.DAT.** These files can be loaded into **REGEDT32.EXE** using the **REGISTRY | LOAD HIVE** menu command.

1. Make the **HKEY_USERS** window active, and click on **HKEY_USERS**. Using the **LOAD HIVE** command on the **REGISTRY** menu, find the appropriate hive. When prompted for the key name, use the username you are editing.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2. Take ownership of the key **ODBC** and its subkeys as was done in the preceding steps. The key will be found in the following location:
   HKEY_USERS
   USERNAME
   SOFTWARE
   ODBC
   ODBC.INI
   ODBC
3. Set the value **TRACE** to **0**. The **TRACE** value can be found under the following Registry key:
   HKEY_LOCAL_MACHINE
   USERNAME
   SOFTWARE
   ODBC
   ODBC.INI
   ODBC
4. Set the value **TRACEDLL** to an empty string. The **TRACEDLL** value can be found under the following Registry key:
   HKEY_LOCAL_MACHINE
   USERNAME
   SOFTWARE
   ODBC
   ODBC.INI
   ODBC
5. Set the permissions for Authenticated Users to **READ** on the **ODBC** key.
6. Remove explicit permissions on the **ODBC** key for any non-administrative users.
7. Unload the hive you just loaded.

In addition, System Administrators and the application developers must also understand how a specific ODBC implementation may affect security. Some implementations may not be suitable for crossing a firewall. However, many implementations use a single, configurable, TCP/IP socket that may be passed through a firewall on a well-known port number.

☐ **LM authentication should be disabled on all Windows NT servers**. (Note that this means that Windows 95 or Windows 98, or any earlier versions of Windows, should not be used as clients.) see Q147706

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Control\lsa
Name:	LMCompatabilityLevel
Type:	REG_DWORD
Value:	4 *

* This causes only NTLM (v1 or 2) to be accepted

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Reason: Lm authentication can allow the capture of password hashes with a packet sniffer. These hashes can then be placed into password cracking tools such as l0phtcrack to extract the passwords. In an all NT environment you can force the system to use only NTLMv2 which is more secure than the older LM hash.

Risk: Requiring NTLMv2 will cause clients using win9x to be unable to connect as they do not support NTLMv2. You can however install the Directory services client from Windos2000 server in conjunction with the 128 bit version of Internet Explorer 4 or 5 to add NTLMv2 128 bit support. Be sure to test compatibility before requiring this setting. See Q239869 about enabling NTLM support on Win9x

Dsclient is located on the Windows 2000 Cd-Rom in \Clients\Win9x\dsclient.exe

☐ **Activate port filtering and only allow needed ports to be unobstructed**

Reason: Use TCP/IP port filtering to block all outbound ports not specifically needed by the web server. The specifics ports will depend on your specific implementation, however you should conceder-disallowing UDP if possible. UDP is connectionless and therefore susceptible to spoofing.

Risk: Blocking ports 135,137,138, and 139 will disable any communication between servers and will also break Microsoft Site Server 3.0 content deployment which is dependant on NetBIOS communications. Many major backup software packages also require NetBIOS communications

☐ **AEDebug key is removed from registry**

Hive:	HKEY_LOCAL_MACHINE
Key:	\software\Microsoft\windowsnt\curentversion\aedebug

Reason: The AEDebug key controls what files are called when an error requiring debugging occurs. It has been found that if you add any file to this registry key that it will be executed with elevated privileges when an error occurs. If you remove the key be sure to make an exported copy first. This way if it is ever required for troubleshooting it can be temporarily added back to the system.

Risk: This will disable Dr. Watson. If you start having application errors you may find it necessary to add the key back to be able to generate Dr. Watson logs.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

☐ **Add Syn Flood protection to the TCP/IP stack**

This setting applies to a system with service pack 5 or higher installed

Hive:	**HKEY_LOCAL_MACHINE**
Key:	**\System\CurrentControlSet\Services\TCPIP\ parameters**
Name:	**SynAttackProtect**
Type	**REG_DWORD**
Value:	**2**

Reason: an attacker could launch a Syn flood attack that can cause a system to become unresponsive as all available resources are attempting to respond to uncompleted TCP/IP handshake requests. The value above will prevent the driver Afd.sys from allocating any resources to a TCP/IP connection until the 3 way handshake is completed. This is documented in Microsoft Knowledge Base article Q142641

Risk: While providing extra protection this setting can slow connections to the system slightly since resources are only allocated after the 3 way handshake is completed. Test the effect on your webserver connections before implementation into a production environment. See the Microsoft article Q183859 for more information.

☐ Enable NetBIOS to open TCP & UDP ports for exclusive access

Reason: It is a TCSEC C2 requirement that an unprivileged user mode application should not be able to listen to TCP and UDP ports used by Windows NT services. This setting will prevent User Applications from attaching to service ports.

Hive	HKEY_LOCAL_MACHINE\SOFTWARE
Key	\CurrentControlSet\Services\NetBT\Parameters
Type	Add new REG_DWORD value named EnablePortLocking
Value	1

Risk: This setting can interfere with application access to the network. Careful testing is required before implementation.

Reference: Microsoft Windows NT C2 Configuration Checklist

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

☐ **Restrict access to Null Session Pipes**

Hive:	**HKEY_LOCAL_MACHINE**
Key:	**System\CurrentControlSet\Services\LanmanServer\ Parameters**
Name:	**NullSessionPipes**
Type	**REG_MULTI_SZ**
Value:	**Remove all possible values**

Reason: A named pipe is a programming construct that allows a process on one system to communicate with a process on a separate system. Restricting null session access to pipes will prevent unauthenticated users from connecting to processes.

Risk: Deciding which entries in the list can be removed is a trial and error situation, which requires careful testing on a non-production server. There is no one list that will be true for all sites.

Reference: Microsoft Articles Q124184, Windows NT C2 Configuration Checklist

☐ **SMB Signing**

SMB signing is an additional authentication feature introduced in SP3. If enabled it requires all SMB traffic between machines be signed for mutual authentication. If it is enabled in "Require traffic to be signed" mode, then a client that is not able to sign it's SMB traffic will be unable to connect.

Hive:	HKEY_LOCAL_MACHINE
Key:	System\CurrentControlSet\Services\LanManServer\Parameters
Name:	`EnableSecuritySignature` Or RequireSecuritySignature
Type:	REG_DWORD
Value:	1

Risk: If SMB signing is enabled Win9x clients will be unable to connect to the machine. There is also up to a 15% overhead for SMB signing.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Reference: Microsoft article Q161372

User Account Options:

☐ **Rename the IUSER and IWAM accounts**

Reason: Hackers know that the Iwam account typically has extra privilege and it is a default account so it is likely to be present. This makes it a good candidate for brute force password guessing.

IIs Specific Options:

☐ **Disable IP address in content-location**
Run the cscript program that is located in the AdminScripts directory:
adsutil set w3svc/usehostname true

Reason: in its response the web server will send the IP address rather than the domain name in URL strings. If you are using NAT based firewalls this is information you probably do not want to be handing out on your network layout. This setting causes the web server to send the domain name rather than the IP address.

Reference: Microsoft Article Q218180

☐ **Use DNS/IP address filtering if Applicable**

Reason: If this site is not publicly available restricting where connections can come from limits your exposure to attacks from outside sources.

Risk: Domain name filtering is slow and imposes a great deal of overhead on your webserver as it has to reverse lookup all connection attempts.

Note: these are not foolproof settings, spoofed addresses will fool these filters. They are a limiting factor but not an ultimate source of security.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

☐ **Disallow IIS remote administration**

Reason: remote administration allows anyone who is able to connect to that address/port to manage a webserver. For maximum security require a Interactive logon to administer the webserver.

Auditing Options:

☐ Full Privilege Auditing

When files are being backed up, Windows NT checks to ensure that the user performing the backup has the Back Up Files and Directories special right each time the backup program attempts to copy a file to the backup media. In the same way, NT checks for the Restore Files and Directories right for each file that is being restored from backup. Obviously, if Windows NT were to record an audit event each time those rights were invoked, thousands of events would be recorded during a routine backup. Because this would flood the security log with event records that most often would be of little value for maintaining system security, Windows NT does not normally record audit events for the use of these rights, even when success auditing of Use of User Rights is enabled in the system user rights policy.

To audit the use of these rights, add the following registry key

Hive:	HKEY_LOCAL_MACHINE\System
Key:	\CurrentControlSet\Control\Lsa
Name:	FullPrivilegeAuditing
Type:	REG_BINARY
Value:	1

The changes take effect the next time the computer is started. You might should also update the Emergency Repair Disk to reflect these changes.

Note The *use* of the following rights is never audited, even when the FullPrivilegeAuditing Registry entry is set to 1. However, the *assignment* of these rights, during logon, is audited.

- Bypass traverse checking (SeChangeNotify)
- Generate security audits (SeAuditPrivilege)
- Create a token object (SeCreateTokenPrivilege)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Debug programs (SeDebugPrivilege)
- Create a new security context for a new logon (AssignPrimaryToken)

Risk: The Full Privilege Auditing setting will rapidly fill the event log, if it is combined with the CrashOnAuditFail setting you can cause a server to shutdown

☐ Crash On Audit Failure

The CrashOnAuditFail registry entry directs the operating system to crash (shutdown abnormally and display a blue screen) when the audit log is full. This assures that no auditable activities, including security violations, occur while the system is unable to log them. To enable CrashOnAuditFail, use the Registry Editor to create the following Registry key value:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	\CurrentControlSet\Control\Lsa
Name:	CrashOnAuditFail
Type:	REG_DWORD
Values:	1 Crash if the audit log is full. 2 (This value is set by the operating system just before it crashes due a full audit log. While the value is 2, only the administrator can log on to the computer. This value confirms the cause of the crash. To reset, change this value back to 1.)

Risk: any time the log fills you have an abnormal system shutdown. This can be a potential avenue for Denial of Service since anything that triggers a event being generated can be used to cause a shutdown.

Reference: Microsoft Q140058

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Bibliography:

Microsoft's Security Website Http://www.microsoft.com/security

Microsoft's Checklist for securing an IIS 4.0 Webserver
Http://www.microsoft.com/technet/security/iischk.asp
Redmond Washington: Microsoft, 15 March 2000

Windows NT C2 Configuration Checklist
Microsoft TechNet

The Internet Information Server Resource kit
Redmond Washington: Microsoft Press, 1998

Braginski, Leonid; Powell, Matthew. *Running Microsoft Internet Information Server*
Redmond Washington: Microsoft Press, 1998

The Nt Server 4.0 Resource Kit
Redmond Washington : Microsoft Press

Jason Fossen and Jennifer Kolde; *Securing Windows NT, Step-by-Step, Parts 1-3*
Sans Network Security 2000 :2000

Sans Securing NT Server-Step by Step Guide Version 2.15
The Sans Institute, 1999

Jumes, James G., et. al. *Microsoft Windows NT 4.0 Security, Audit, and Control.*
Redmond Washington: The Microsoft Press, 1999.

McClure, Stuart; Scambray, Joel; Kurtz, George. *Hacking Exposed, Network Security Secrets and Solutions*. Berkeley: Osborne/McGraw-Hill, 1999.

Heckendorn, Sherri . *Sans Giac paper (untitled)*
Sans Giac Website, 1999

Michelli, Don. *Practical Assignment for SANS Security DC 2000 paper*
Sans Giac Website, 1999

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.