Global Information Assurance Certification Paper

Web Server Auditing

Windows NT and Internet Information Service 4.0

Level Two Securing Windows
GCNT Practical Assignment v1.6
Option 1 – Developments in auditing Windows NT 4.0

By: *Chris Young*
Date: April 4, 2001

Abstract

This document, written to complete requirements for the GIAC certification for Windows NT, is intended as a guide to performing system security audits of a Content Web Server. It outlines some of the corrective measures that should be taken in order to secure and protect the server from attackers.

Table of Contents

ABSTRACT 1

TABLE OF CONTENTS 2

INTRODUCTION 3

ASSUMPTIONS 4

WEB SERVER CHECKLIST 5

- DOMAIN CONTROLLER TYPE 6
- NT FILE SYSTEM (NTFS) FORMAT 7
- INSTALL ONLY NECESSARY OPTION PACK APPLICATIONS 8
- SERVICE PACKS AND HOTFIXES 9
- PROTECT FILES AND DIRECTORIES 10
- ADMINISTRATOR ACCOUNT 12
- ALLOW NETWORK ONLY LOCKOUT OF ADMINISTRATOR ACCOUNT 13
- REMOVE AND/OR DISABLE ALL UNNECESSARY LOCAL ACCOUNTS 14
- USER RIGHTS MEMBERSHIP 15
- MOVE POTENTIALLY DANGEROUS FILES 17
- APPLY STRONG ENCRYPTION TO SECURITY ACCOUNT MANAGER (SAM) 17
- DISABLE IP ROUTING 18
- UNBIND WINS CLIENT FROM TCP/IP 19
- USE LOCAL TCP/IP FILTERING TECHNIQUES 20
- USE APPROPRIATE REGISTRY ACCESS CONTROL LISTS 21
- REMOVE ALL SAMPLE APPLICATIONS AND RESOURCE KIT TOOLS 23
- REMOVE THE IISADMPWD VIRTUAL DIRECTORY 24
- SET APPROPRIATE WEB SPACE PERMISSIONS 25
- SET APPROPRIATE AUTHENTICATION METHODS 26
- AUDITING 27
- REMOVE OS/2 AND POSIX SUBSYSTEMS 30
- REMOVE UNUSED ISAPI EXTENSIONS MAPS 31
- REMOVE UNUSED ODBC/OLE-DB DATA SOURCES AND DRIVERS 32
- DISABLE NON-REQUIRED SERVICES 33
- DISABLE IP ADDRESS IN CONTENT LOCATION 34
- ADD SYN FLOOD PROTECTION 35
- RESTRICT ANONYMOUS NETWORK ACCESS 36
- REMOVE REMOTE DATA SERVICE (RDS) SUPPORT 37
- SHUT OFF NTFS 8.3 NAME GENERATION 38
- REMOVE SHUTDOWN BUTTON FROM LOGON DIALOG 39
- CLEAR PAGING FILE AT SYSTEM SHUTDOWN 40
- AVOID THE NETWARE DLL TROJAN HORSE 41
- RESTRICT FLOPPY DRIVE AND CD-ROM DRIVE ACCESS TO INTERACTIVE ONLY 42

CONCLUSION 43

CREDITS AND REFERENCES 44

Introduction

System security auditing allows for proper evaluation of the current security measures against a security policy and identifies vulnerabilities that need to be addressed.

There are numerous steps that can be taken to secure a Web Server, thereby minimizing the vulnerabilities inherent in an "out-of-the-box" Windows NT system. This document describes those vulnerabilities, explains the risks associated with the vulnerability, details the best practices around the vulnerability, and audits the system against the vulnerability.

Before conducting an audit, a comprehensive security policy must be in place in order to assess compliance or non-compliance of targeted systems. This audit document assumes that a security policy is being adhered to and all modifications, described in the audit, to the system are policy-compliant.

Throughout this audit, best practices are described for particular vulnerabilities, and in most cases, the audit enforces these corrective measures. Of course some of the corrective measure may in fact disable proper functionality of the system. In these cases, the auditor must note the difference and explain why the best practices could not be adhered to.

This audit document contains information about editing the registry. Before you edit the registry, make sure you understand how to restore it if a problem occurs. For information about how to do this, view the "Restoring the Registry" Help topic in Regedit.exe or the "Restoring a Registry Key" Help topic in Regedt32.exe.

Assumptions

This document assumes the following items:

- The OS is Windows NT version 4.0.
- The Web Server is IIS version 4.0.
- The Web Server is located in a secure physical environment.
- Limited access to physical environment.
- Web Server is located in a DMZ (protected by a Firewall and Network Address Translation).
- System is only used as Web server for content presentation.
- System uses LMHOST and HOST files for protected name resolution.
- System uses an external DNS server for other name resolution.
- Company wide security policy exists and the web servers are addressed under those policies.
- System is backed up locally with a direct attached backup device.
- Backup media is transported securely and is also securely stored both on-site and off-site.
- All new applications and content are first tested in a development environment before being installed on the web server.
- Audit logs are checked.
- Server will have a static IP address.
- The auditor either has previous experience in NT administration or the assistance of an NT administrator during the review process.

Web Server Checklist

Auditing Windows NT and Internet Information Service 4.0

Server Name: _____

Asset Number: _____

Location: _____

Set-up Date: _____

Set-up By: _____

Audit Date: _____

Audited By: _____

Notes: _____

_____

_____

_____

_____

Procedures:

During this audit mark all yellow boxes with a check mark (P) if the audit results are correct. If the results differ, mark an X in the yellow box (O) and then describe why the results vary from the policy or the best practices.

DOMAIN CONTROLLER TYPE

Description

- The Web Server being a system that is in the DMZ does not need to be a member of a domain or a Domain Controller. A standalone server does not establish a NetLogon channel to any domain controllers thus uses only local accounts.

Risks

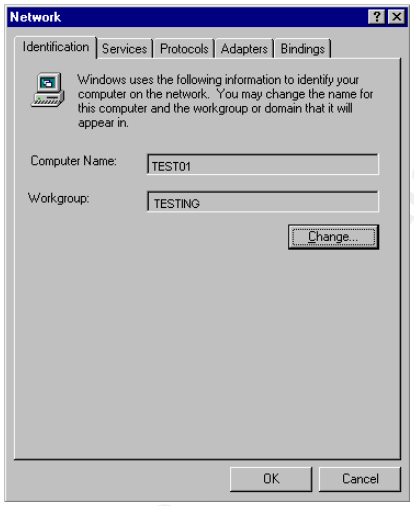
- Having the server as a Member server or a Domain Controller requires that NetBIOS communication port 136,138, and 139 be open. There are numerous vulnerabilities with the NetBIOS ports open.
- Minimize the possibility of having the domain user accounts exposed.

Best Practices

- Implement the server as Standalone. Block all NetBIOS ports with a firewall.

Audit

- Open `Contol Panel | Network | Identification` and check to see if server is a member of a Workgroup. It should only be a member of a Workgroup, not a Domain. See diagram below.



Results

☐ Server is Standalone as per policy.

Notes _____

_____

_____

NT File System (NTFS) Format

Description

- Windows NT supports two types of file systems, FAT and NTFS. The use of NTFS File System allows the use of Access Control Lists, Auditing and provides greater protection of data.

Risks

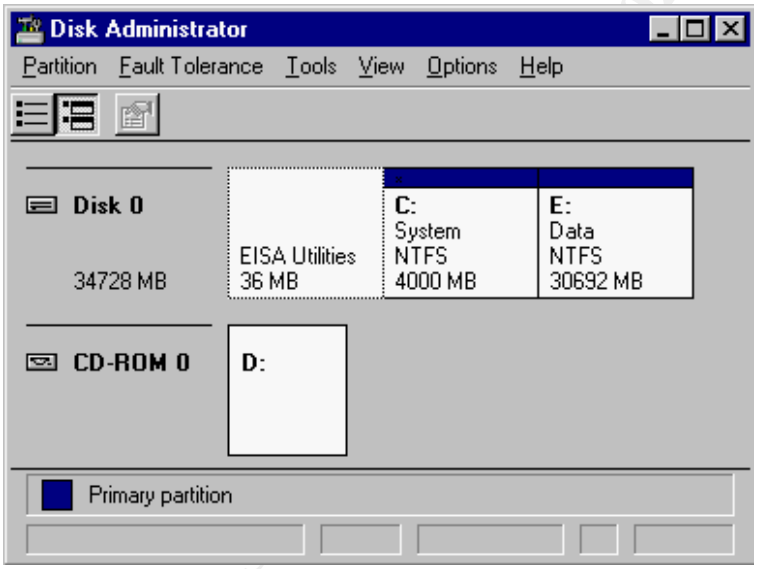
- Windows NT does not support file system security (permissions) with FAT.
- FAT does not support Auditing, thus no record of a possible intrusion.

Best Practices

- Use NTFS on all partitions with proper Access Control Lists (see Protect Files and Directories section for details).

Audit

- Open the Windows Disk Administrator and check the properties of all partitions. See diagram below.



Results

All Disk Partitions are NTFS as per policy.

Notes _____

_____

_____

INSTALL ONLY NECESSARY OPTION PACK APPLICATIONS

Description

- Contained within the Option Pack for Windows NT is not only IIS but also a lot of other tools and applications. It is not necessary to install all of the components within the Option Pack.

Risks

- Some of the components within the Option Pack contain vulnerabilities that could allow an attacker access to the web site content.

Best Practices

- Since this is a Web Server that displays content and content is updated by means other than FrontPage, only install the minimal components required.

Audit

- Use the Add/Remove Programs Manager in the Control Panel; select 'Windows NT 4.0 Option Pack'; select 'add/remove…'; select 'next'; select 'add/remove'; now check to make sure the following components are NOT installed.
  - Certificate Server
  - FrontPage 98 Server Extensions
  - Internet Connection Service for RAS
  - The following subcomponents under Internet Information Server (IIS)
    - File Transfer Protocol (FTP) Server
    - Internet NNTP Service
    - Internet Service Manager (HTML)
    - SMTP Service
    - World Wide Web Sample Site
  - Microsoft Index Server
  - Microsoft Message Queue
  - Microsoft Script Debugger
  - Microsoft Site Server Express 2.0
  - The following subcomponent under Transaction Server
    - Transaction Server Development
  - Visual InterDev RAD Remote Deployment Support
  - Windows Scripting Host

Results

☐ The listed Option Pack components above are not installed as per policy. If any additional components are installed explain why below.

Notes _____

_____

SERVICE PACKS AND HOT FIXES

Description

- Service Packs include updates, system administration tools, drivers, and additional components." (Microsoft Knowledge Base Article ID: Q152734).
- Hot Fixes address a particular issue and provide a work around or a fix.
- 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 www.microsoft.com/technet/security/current.asp for the latest security risks and links to current patches.

Risks

- Without the latest Service Pack or Hot Fix, the system is exposed to published and maybe even unpublished security vulnerabilities.

Best Practices

- Systems administrators must continually practice due diligence and be on top of the latest developments via Microsoft security email alerts, newsgroup discussion forums, or sites that post the latest Windows vulnerabilities.
  - Subscribe to the Microsoft Security notification service at www.microsoft.com/technet/security/notify.asp and receive the latest bulletins from Microsoft by email.
  - Also subscribe to other email notification services like SANS at www.sans.org/sansnews. Regularly check for updated information.
- Test Service Packs and Hot Fixes on a non-production system as soon as practical. Deploy to production once the Service Pack or Hot Fix is determined to be stable and compatible with existing systems and applications.
- Note: Installing Service Packs and Hot Fixes will generally require a reboot of the system.

Audit

- Use WINVER.EXE to determine the level of Service Pack.
- Use the add/remove programs manager from Control Panel to determine which Hot Fixes are applied and check against Microsoft Security Bulletins at www.microsoft.com/technet/security/current.asp.

Results

☐ Service Pack 6a for NT Installed as per policy.

☐ All relevant Hot Fixes for both NT Server and IIS 4.0 Installed. Make note of all Hot Fixes applied to date below. Keep this list up to date for auditing purposes.

Notes _____

PROTECT FILES AND DIRECTORIES

Description

- The Windows NT file system contains many areas of critical security files that need to be further protected from the default settings.

Risks

- Attackers could use the Anonymous or equivalent account to gain access to critical security files for destruction or further attacks.

Best Practices

- Ensure that the following maximum ACL's are set on the file system.
- In the below table, "Installers" refers to any accounts with privileges to install application or system software. "Authenticated Users" refers to any account that can authenticate to the server (i.e. IUSR_ServerName). "Server Operators" refers to any account that administers the server.

Directory or file	Suggested Max Permissions
C:\	Installers: Change Authenticated Users: Read Server Operators: Change
files	Installers: Change Authenticated Users: Read Server Operators: Change
IO.SYS, MSDOS.SYS	(none)
BOOT.INI, NTDETECT.COM, NTLDR	(none)
AUTOEXEC.BAT, CONFIG.SYS	(none)
C:\TEMP	Authenticated Users: (RWXD)*(NotSpec)
C:\WINNT\	Installers: Change Authenticated Users: Read Server Operators: Change
files	Authenticated Users: Read Server Operators: Change
Netlogon.chg	(none)
\WINNT\config\	Installers: Change Authenticated Users: Read Server Operators: Change
\WINNT\help\	Installers: Change Authenticated Users: Add & Read Server Operators: Change
*.GID, *.FTG, *.FTS	Authenticated Users: Change
\WINNT\inf\	Installers: Change Authenticated Users: Read
*.ADM files	Authenticated Users: Read
*.PNF	Installers: Change Authenticated Users: Read Server Operators: Change
\WINNT\media\	Installers: Change Authenticated Users: Read Server Operators: Change

*.RMI	Authenticated Users: Change
\WINNT\profiles\	Installers: Add&Read Authenticated Users: (RWX)*(NotSpec)
..\All users	Installers: Change Authenticated Users: Read
..\Default	Authenticated Users: Read
\WINNT\repair\	(none)
\WINNT\system\	Installers: Change Authenticated Users: Read Server Operators: Change
\WINNT\System32\	Installers: Change Authenticated Users: Read Server Operators: Change
files	Authenticated Users: Read Server Operators: Change
$winnt$.inf	Installers: Change Authenticated Users: Read Server Operators: Change
AUTOEXEC.NT, CONFIG.NT	Installers: Change Authenticated Users: Read Server Operators: Change
cmos.ram, midimap.cfg	Authenticated Users: Change
localmon.dll, decpsmon.*, hpmon.*	Installers: Change Authenticated Users: Read Server Operators: Change
\WINNT\System32\config\	Authenticated Users: List
\WINNT\System32\drivers\ (including \etc)	Authenticated Users: Read
\WINNT\System32\viewers	Authenticated Users: Read Server Operators: Change
C:\...*.EXE, *.BAT, *.COM, *.CMD, *.DLL	Authenticated Users: X

Audit

- Use the File Explorer's security tab in the properties of the above list to check for the proper security level.

Results

The ACL's are set as per above table. Note any differences from the above table and give an explanation to why.

Notes _____

_____

_____

ADMINISTRATOR ACCOUNT

Description

- The Administrator account is built into Windows NT. It cannot be disabled or at the console.

Risks

- The Administrator account presents a well-known objective for hackers to crack and gain access to system with Administrator privilege.

Best Practices

- Rename the account to a non-obvious name and remove the Description field.
- Establish a decoy account named "Administrator" with no privileges and disable this account. Scan the event log regularly looking for attempts to use this account.
- Use very strong password of 14 characters with at least one extended ASCII character.

Audit

- Open User Manager and check the accounts for the above settings.

Results

☐ Administrator account renamed as per policy.

☐ Administrator account has strong password as per policy.

☐ The decoy administrator account does exist and is locked.

Notes _____

_____

_____

ALLOW NETWORK ONLY LOCKOUT OF ADMINISTRATOR ACCOUNT

Description

- By default the administrator account cannot be locked out by too many wrong password attempts. A tool in the Microsoft Windows Resource Kit called Passprop.exe can change this default so that the administrator account will lock out if too many attempts are made across the network, but will remain unlocked at the console.

Risks

- An attacker could attempt to guess the administrator account using brute force or dictionary password attacks.

Best Practices

- Run the following command from the Resource Kit to allow the administrator account to be locked out across the network.
  - PASSPROP.EXE /ADMINLOCKOUT

Audit

- Use the Passprop.exe command to identify the current setting, see below.
  - ```
    C:\>passprop
    Password must be complex
    The Administrator account may be locked out except for interactive
    logons on a domain controller.
    ```

Results

☐ The administrator account is set to allow lockout as per policy.

Notes _____

_____

_____
    ```

REMOVE AND/OR DISABLE ALL UNNECESSARY LOCAL ACCOUNTS

Description

- Windows NT by default includes a Guest user account, which on servers is disabled on install; this account is unnecessary make sure it is disabled.
- All accounts that are unnecessary should be removed.

Risks

- These accounts could be used as a stepping stone to get further into the system by a hacker.

Best Practices

- Remove all unnecessary accounts and disable to guest account.
- Give the Guest account a strong password just in case it is ever unlocked by mistake.
- Only strong password protected administrator accounts, the disabled guest account, and the IUSR, IWAN accounts should exist.

Audit

- Use User Manager to view Local Accounts and check for above best practices.

Results

☐ Meets best practice as per policy, if there are exceptions note them below.

Notes _____

_____

_____

USER RIGHTS MEMBERSHIP

Description

- In Windows NT the User Rights are assigned by default to the built-in users, but a number of changes need to be made to limit the risks of exposure.

Risks

- Improper setting of User Rights could allow an intruder to do a number of attacks against the system.

Best Practices

- Use User Manager to restrict the use of user rights as shown in the table below.

User Right	Membership
Access this computer from network	(No one) **Since this is a standalone server, no access is required via the network.**
Act as part of the operating system	(no one) **Do not assign to any user**.
Add workstations to domain	Domain Admins
Back up files and directories	Trusted users (e.g. the Backup Operators group)
Bypass traverse checking	Authenticated Users
Change the system time	Trusted users (e.g. Server Operators)
Create a pagefile	Trusted users (e.g. Server Operators)
Create a token object	(no one) **Do not assign to any user**.
Create permanent shared objects	(no one)
Debug programs	(no one) **This right is not auditable and should not be assigned to any user, including system administrators.**
Force shutdown from a remote system	Trusted users (e.g. Server Operators)
Generate security audits	(no one) **Do not assign to any user.**
Increase quotas	Trusted users (e.g. Server Operators)
Increase scheduling priority	Trusted users (e.g. Server Operators)
Load and unload device drivers	Trusted users (e.g. Server Operators)
Lock pages in memory	(no one)
Log on as a batch job	Trusted users (as needed)
Log on as a service	Trusted users (as needed)
Log on locally	Trusted users (as needed)
Manage auditing and security log	Trusted users (e.g. Domain Admins)
Modify firmware environment values	Trusted users (e.g. Domain Admins)
Profile single process	Trusted users
Profile system performance	Trusted users
Replace a process level token	(no one) **Do not assign to any user.**
Restore files and directories	Trusted users (e.g. Backup Operators)
Shut down the system	Trusted users (e.g. Server Operators)
Take ownership of files or other objects	trusted users (e.g. Domain Admins)

Audit

- Use User Manager to check the User Rights as shown in the above table.

Results

☐ All User Rights are set as in table above as per policy. If any differences exist, note them below and explain why.

Notes _____

_____

_____

MOVE POTENTIALLY DANGEROUS FILES

Description

- Some executable files on NT can provide information that can lead to further exposure. The files, by default, exist in the system path and can be executed anywhere.

Risks

- Attackers could trick the web server into executing known files from know locations or from the system path.

Best Practices

- Move to a secure location other than default and audit access to the following list of files:
  - ARP.EXE
  - AT.EXE
  - ATSVC.EXE
  - CACLS.EXE
  - CMD.EXE
  - CSCRIPT.EXE
  - DEBUG.EXE
  - EDIT.EXE
  - EDLIN.EXE
  - FINGER.EXE
  - FTP.EXE
  - IPCONFIG.EXE
  - ISSYNC.EXE
  - NBTSTAT.EXE
  - NET.EXE
  - NETSH.EXE
  - NETSTAT.EXE
  - NSLOOKUP.EXE
  - PING.EXE
  - POLEDIT.EXE
  - POSIX.EXE
  - QBASIC.EXE
  - RCP.EXE
  - RDISK.EXE
  - REGEDIT.EXE
  - REGEDT32.EXE
  - REGINI.EXE
  - REGSRV32.EXE
  - REXEC.EXE
  - ROUTE.EXE
  - RSH.EXE
  - RUNAS.EXE
  - RUNONCE.EXE
  - SECFIXUP.EXE
  - SYSKEY.EXE
  - TELNET.EXE
  - TFTP.EXE
  - TRACERT.EXE
  - TSKILL.EXE
  - WSCRIPT.EXE
  - XCOPY.EXE
- Do not include these files in the PATH environment variable.
- Do not allow access from any of the following accounts:
  - IUSR_computername, IWAM_computername, System, or any account with local logon rights.

Audit

- Check for location of files and use explorer to check for audit settings.

Results

☐ Files are moved and are audited for access as per policy. Make note of any other files that are moved to this secure location below.

Notes _____

_____

_____

APPLY STRONG ENCRYPTION TO SECURITY ACCOUNT MANAGER (SAM)

Description

- The Security Account Manager (SAM) database stores password hashes for domain and local computer accounts.

Risks

- An attacker who gains access to the SAM database files (either from the server itself, the server's emergency repair disk, over the network, or a backup tape) can use a password-cracking tool to extract passwords from the hashes.

Best Practices

- Use the SYSKEY tool to encrypt the SAM database, this will make it more difficult for an unprivileged attacker to use password-cracking tools against your stored password hashes.
- *Warning* - Before you install SYSKEY, make sure to update your server's emergency repair disk. After installing SYSKEY, make a second ERD using a new, separate floppy. Do not attempt to use the pre-SYSKEY ERD to restore your system once SYSKEY is installed.
- Note: Encrypting the SAM does NOT protect password hashes that are stored in cache memory or in transit over the network.
- For details on how to install and use SYSKEY see Microsoft Knowledge Base article Q143475.

Audit

- Run SYSKEY.EXE to see current setting of encryption on SAM. See below.

Results

Strong Encryption is applied to SAM as per policy.

Notes _____

_____

_____

DISABLE IP ROUTING

Description

- IP routing in Windows NT allows traffic from one interface to be routed through to another interface. Since in most cases a Web server is located in a DMZ and might have the other interface connected to the private side, it is necessary to disable the routing.

Risks

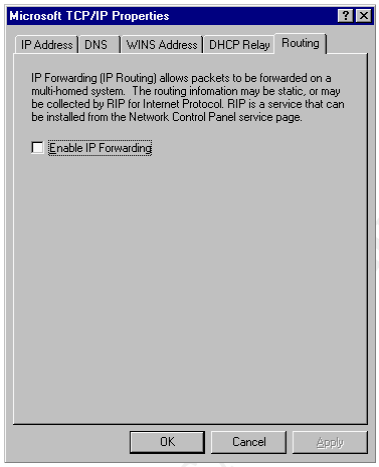
- Risk of passing data between the intranet and Internet or two interfaces on the system.

Best Practices

- Turn off IP Routing.
  - Open the Control Panel | Network | Protocols | TCP/IP Protocol | Properties | Routing and clear the Enable IP Forwarding check box.

Audit

- Open the Control Panel | Network | Protocols | TCP/IP Protocol | Properties | Routing and make sure the Enable IP Forwarding check box is clear. See diagram below.



Results

IP Routing is disabled as per policy.

Notes _____

_____

_____

UNBIND WINS CLIENT FROM TCP/IP

Description

- The "WINS client (TCP/IP)" represents NetBIOS Over TCP/IP. NetBIOS is the protocol Windows NT uses to communicate with other Windows OS's. HTTP and FTP do not use NetBIOS.

Risks

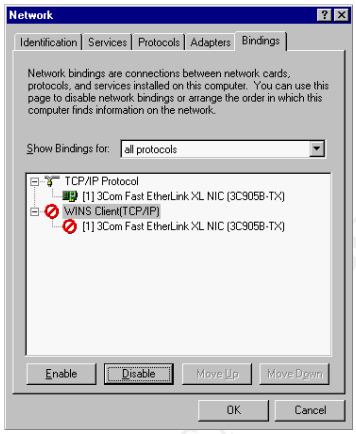
- Hackers could access machine information using tools like NBTSTAT.
- Denial of service attacks against the protocol.
- NetBIOS specific exploits.
- Access to shared folders and printers.

Best Practices

- Unbind NetBIOS from TCP/IP. To unbind use the bindings tab of the Network Manager in the Control Panel.
- Unbind all other unnecessary protocols.

Audit

- Use the Network Manager from the Control Panel to check for the disabled NetBIOS. See diagram below.



Results

☐ NetBIOS is disabled as per policy.

☐ Other protocols beside TCP/IP are disabled. Make note of these below.

Notes _____

_____

USE LOCAL TCP/IP FILTERING TECHNIQUES

Description

- Windows NT supports TCP/IP filtering for TCP and UDP ports. IIS supports filtering on an IP address level per web site. Rules for IP addresses are defined for single addresses, range of addresses based on network ID, and subnet mask, or domain names.

Risks

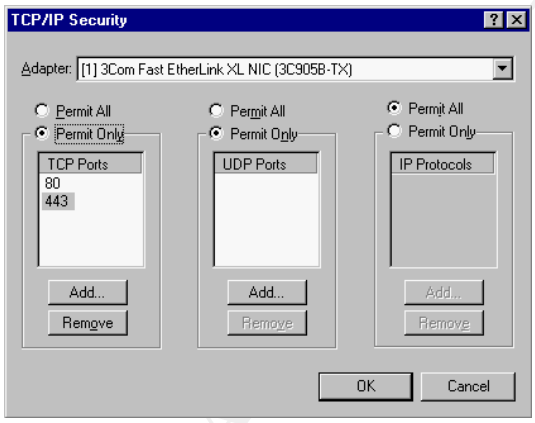
- If an attacker enters the DMZ by getting past the firewall, the web server is fully open to attack without it's own blocking rules.

Best Practices

- Use IP filtering where possible on the web site. Use port TCP/IP filtering to allow only TCP ports 80 and 443 inbound. No UDP ports.
  - Go to Control Panel | Network | Protocols | TCP/IP | Advanced | Enable Security | Configure.

Audit

- Open Network manager in Control Panel and look for port filtering. The setting should allow only TCP ports 80 and 443, no UDP ports. See diagram below.



Results

Ports 80 and 443 are the only IP address ports allowed as per policy. If IP address filters are in place on the web site, make note of it below.

Notes _____

_____

_____

USE APPROPRIATE REGISTRY ACCESS CONTROL LISTS

Description

- By default Windows NT registry security (ACL's) are insecure and require changes to tighten security.

Risks

- An attacker could use tools such as REGEDIT.EXE, REGEDT32.EXE and POLEDIT.EXE to access the registries of servers over the Internet or Company Network.
- An untrusted user could plant a Trojan Horse within the registry under "runonce" or "Run" and have it execute.

Best Practices

- Restrict unauthenticated network access to the registry by setting the security permissions (ACLs) on the key below to the Administrators group and the System account.
  - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\winreg
- Change the following registry key from their defaults to those listed below.
  - *Warning:* Unless the table says "Entire tree", change permissions only on the indicated key, not its subkeys.
  - Note: In the table, "Installers" refers to any accounts with privileges to install application or system software.

Key path	Permissions	Notes
\Software	Installers: Change Everyone: Read	Only accounts that can install software should have change rights to this tree.
\Software\Classes	Installers: Add Everyone: Read	Tree needs special treatment because restricting to read access for Everyone may break some applications.
\Software\Microsoft\Windows\CurrentVersion\App Paths	Installers: Change Everyone: Read	Apply to entire tree. At install time this key is empty; set ACLs to prevent its misuse.
\Software\Microsoft\Windows\CurrentVersion\Explorer	Everyone:Read	Apply to entire tree
\Software\Microsoft\Windows\CurrentVersion\Embedding	Installers: Change Everyone: Read	Apply to entire tree
\Software\Microsoft\Windows\CurrentVersion\Run, RunOnce, Uninstall, and AEDebug	Everyone: Read	Apply to all their subkeys
\Software\Microsoft\Windows NT\CurrentVersion\Font*, GRE_Initialize	Installers: Change Everyone: Add	Change only keys that begin with "Font," except FontDrivers, and Gre-Initialize.
\Software\Microsoft\Windows NT\CurrentVersion\Type 1 Installer\Type 1 Fonts	Installers: Change Everyone: Add	

\Software\Microsoft\Windows NT\CurrentVersion\Drivers, Drivers.desc	Everyone: Read	Apply to entire tree
\Software\Microsoft\Windows NT\CurrentVersion\MCI, MCI Extensions	Installers:Change	Apply to entire tree.
\Software\Microsoft\Windows NT\CurrentVersion\Ports	INTERACTIVE: Read Everyone: Read	Apply to entire tree.
\Software\Microsoft\Windows NT\CurrentVersion\WOW	Everyone: Read	Apply to entire tree.
\Software\Windows 3.1 Migration Status	Everyone: Read	Apply to entire tree.
\System\CurrentControlSet\Services\LanmanServer\Shares	Everyone: Read	Apply to entire tree. Prevents users from adding new shares.
\System\CurrentControlSet\Services	Everyone: Read	Apply to entire tree. This setting prevents non-administrators from changing service settings.

Audit

- Use Regedt32.exe to check the above keys for proper permission settings.

Results

☐ Security permissions are set on the 'winreg' key as per policy.

☐ Security permissions are set as described in the above table as per policy.

Notes _____

_____

_____

Remove All Sample Applications and Resource Kit Tools

Description

- Sample web pages and scripts are included with IIS and should be deleted or not installed. Windows NT or IIS resource kits include more samples and provide handy tools for hackers.

Risks

- Numerous exploits exist for the IIS sample pages.
- Sample scripts permit hackers to read arbitrary files from the IIS server.
- Resource Kit tools could potentially be used against you.

Best Practices

- Do not install the samples from the option pack.
- Delete the following directories:
  - \inetpub\iissamples and all subdirectories.
  - \Program Files\Common Files\System\msadc\Samples
  - \inetpub\AdminScripts
- Do not install resource kits. If you need a tool copy only that piece to a secure directory that is not in the PATH.

Audit

- Check for above folders and for the Resource kits.

Results

☐ All samples are removed as per policy.

☐ No Resource Kits on server as per policy.

Notes _____

_____

_____

REMOVE THE IISADMPWD VIRTUAL DIRECTORY

Description

- The IISADMPWD folder is a group of rarely used scripts for changing passwords with IIS 4.0 via the Internet.

Risks

- This group of scripts could allow an attacker to use brute force against the system user accounts.

Best Practices

- Remove the folder, if not used, as shown below:
  - %systemroot%\System32\Inetsrv\IISadmpwd

Audit

- Check for the existence of the %systemroot%\System32\Inetsrv\IISadmpwd directory.

Results

☐ IISadmpwd directory removed as per policy.

Notes _____

_____

_____

SET APPROPRIATE WEB SPACE PERMISSIONS

Description

- IIS uses it's own permissions for controlling what can be done on the web site. There are basically two areas, Access Permissions and Application Permissions. Access Permissions control access to the content and Application Permissions control access to applications (i.e. scripts and executables).

Risks

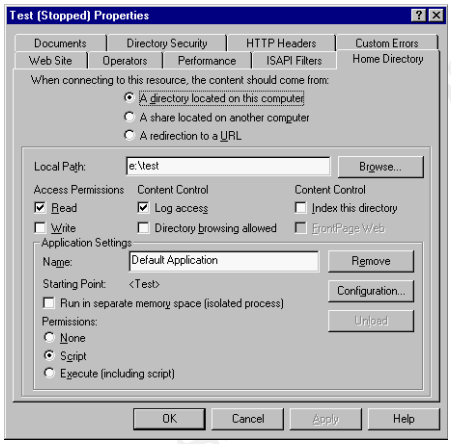
- Having too much access such as Write Access Permission and Execute Application Permission allows an attacker the ability to upload an executable (like a Trojan Horse) and then execute it.

Best Practices

- Use minimum access and applications permissions, like Read, Log Access, and Script.

Audit

- Open the IIS MMC tool | Right-click on site in question | Properties | Home Directory and check the permissions. Permissions should be Read, Log Access, and Script only. See diagram below.



Results

All web sites permission's are set as per above as per policy.

Notes _____

_____

_____

SET APPROPRIATE AUTHENTICATION METHODS

Description

- The following list of authentication schemes is supported by IIS4 in increasing trust.
  - Anonymous
  - Basic
  - Windows NT Challenge/Response
  - Client Certificates
- Since the web site is a content display only site, the anonymous authentication scheme is the only required authentication required.

Risks

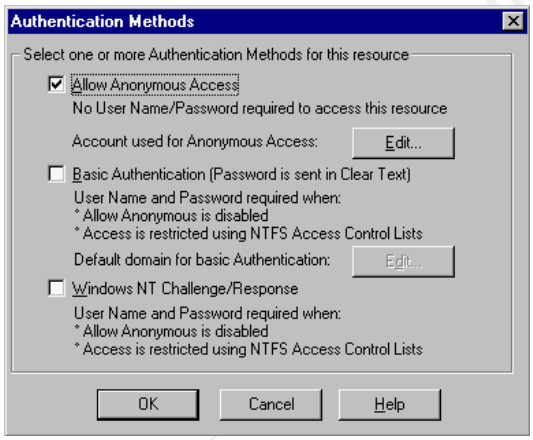
- Using other schemes could potentially lead to the site being cracked by providing the attacker the ability to use brute force to guess an administrator account.

Best Practices

- Use only the anonymous authentication scheme on all web sites.

Audit

- Open the IIS MMC tool | Right-click on site in question | Properties | Directory Security | Edit and verify that anonymous is the only authentication method. See diagram below.



Results

☐ Only anonymous authentication is used on all web sites as per policy.

Notes _____

_____

_____

AUDITING

Description

- Windows NT supports auditing of user and system activities. A default installation of Windows NT does not have auditing enabled. Enabling audit policies enables the documenting and tracking of user and system activities.
- IIS supports auditing of Web and FTP traffic to sites. Changes to the default log settings and locations need to be made to ensure proper tracking and functionality.

Risks

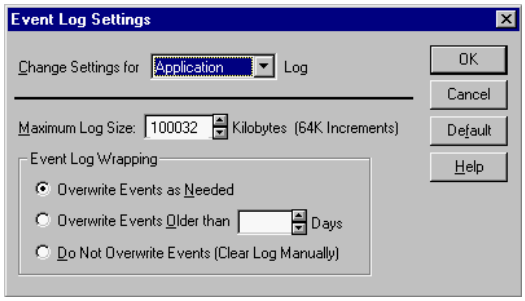
- Without system auditing an attacker could attempt to compromise the system and the administrator would have no way to know about the attack.
- Without the appropriate ACLs on the log files an attacker could change or delete the log files to cover their tracks.

Best Practices

- Ensure system auditing is enabled.
- Ensure the system events are set as follows.

Audit Item		Policy
Logon and Logoff	Success	Enabled
Logon and Logoff	Failure	Enabled
File and Object Access	Success	Disabled
File and Object Access	Failure	Enabled
Use of User Rights	Success	Disabled
Use of User Rights	Failure	Enabled
User and Group Management	Success	Enabled
User and Group Management	Failure	Enabled
Security Policy Changes	Success	Enabled
Security Policy Changes	Failure	Enabled
Restart, Shutdown and System	Success	Enabled
Restart, Shutdown and System	Failure	Enabled
Process Tracking	Success	Disabled
Process Tracking	Failure	Disabled

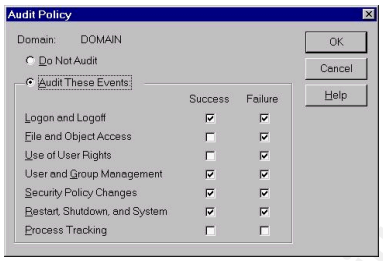
- Note: The options “Use of User Rights” and “Process Tracking” create a large volume of entries in the logs files. Activating both success and failure for both these items can generate a heavy overhead on the server.
- Set maximum size and overwrite interval for audit logs.
  - Open `Event Viewer | Log | Log Settings`, and set a maximum size to a least 100MB and set "Overwrite as required" for all three logs. See diagram on next page.



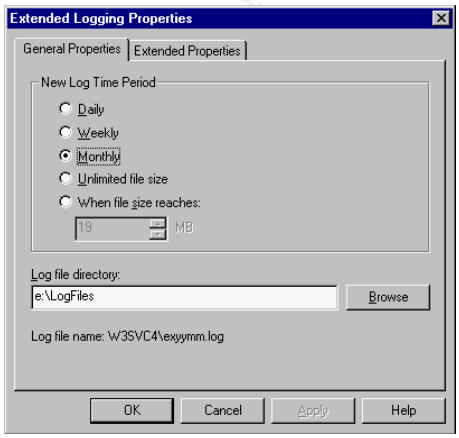
- Use W3C Extended Logging format in IIS for all web and virtual sites.
  - Do this by opening the IIS MMC tool | Right-click on site in question | Properties | Web Site | Enable Logging (W3C Extended Log), then enable all the extended properties.
- The default location of the IIS log files (%systemroot%\system32\LogFiles) needs to be changed to a non-system partition to prevent a DOS attack by filling up the system partition.
- Set the following IIS log file ACLs on the IIS generated log files.
  - Administrators (Full Control)
  - System (Full Control)

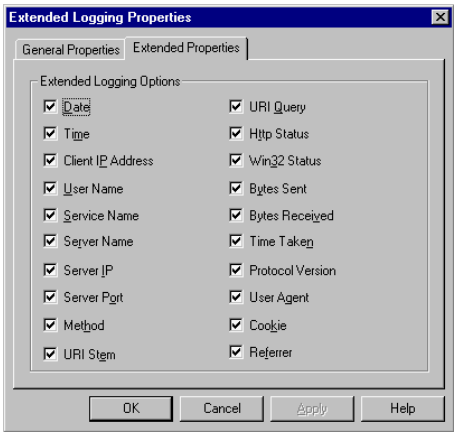
Audit

- Open User Manager | Policies | Audit… and check the system audit policy as shown below.



- Open the IIS MMC tool | Right-click on site in question | Properties | Web Site | properties and check the location of the W3C Extended Logging, then check the extended properties. Should look like the following two diagrams below.





Results

- [ ] System auditing is enabled as per policy.
- [ ] All system audit events are set as per table as per policy.
- [ ] All system audit files have maximum size and overwrite intervals set as described above as per policy.
- [ ] IIS auditing is enabled and all extended properties are enabled as per policy.
- [ ] IIS audit files are moved to non-system partition and proper ACLs applied as per policy.

Notes _____

_____

_____

REMOVE OS/2 AND POSIX SUBSYSTEMS

Description

- The OS/2 and Posix Subsystems are used to provide compatibility with legacy systems.

Risks

- These systems may provide unseen vulnerabilities.

Best Practices

- Disable the OS/2 and Posix Subsystems as described next.
  - Delete all sub keys from:
    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT.
  - Delete Os2LibPath key from:
    HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment.
  - Delete Optional, Posix and OS/2 keys from:
    HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems.
  - Delete the \winnt\system32\os2 directory and all subdirectories.

Audit

- Use REGEDIT.EXE and EXPLORER.EXE to look for the above items.

Results

☐ OS/2 and Posix Subsystems removed as per policy.

Notes _____

_____

_____

REMOVE UNUSED ISAPI EXTENSIONS MAPS

Description

- IIS is preconfigured to support common filename extensions such as .ASP and .SHTM. When IIS receives a request for a file of one of these types the call is handled by or mapped to a DLL.

Risks

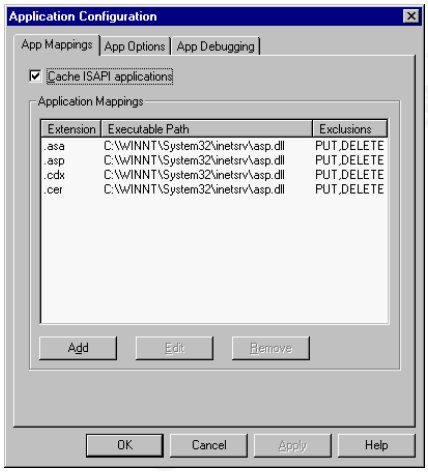
- Extensions are subject to DoS and buffer overflow attacks like any other service.
- Permit an attacker to run arbitrary code on the IIS server.

Best Practices

- Remove all unused and the following ISAPI Extensions from IIS.
  - .htr (Web based password reset)
  - .idc (Internet database connector)
  - .shtm, .shm, .shtml (Server side includes)

Audit

- Check for the above ISAPI Extensions and any unused Extensions (Open the `IIS MMC tool | Right-click on site in question | Properties | Home Directory | Configuration | App Mappings`). The results should look like the following diagram for a typical Web Server.



Results

All unused Extensions and the listed Extensions are removed as per policy.

Notes _____

_____

REMOVE UNUSED ODBC/OLE-DB DATA SOURCES AND DRIVERS

Description

- By default Windows NT will contain a number of sample data sources in the ODBC manager, it will also contain a number of drivers. The samples and unused drivers should be removed.

Risks

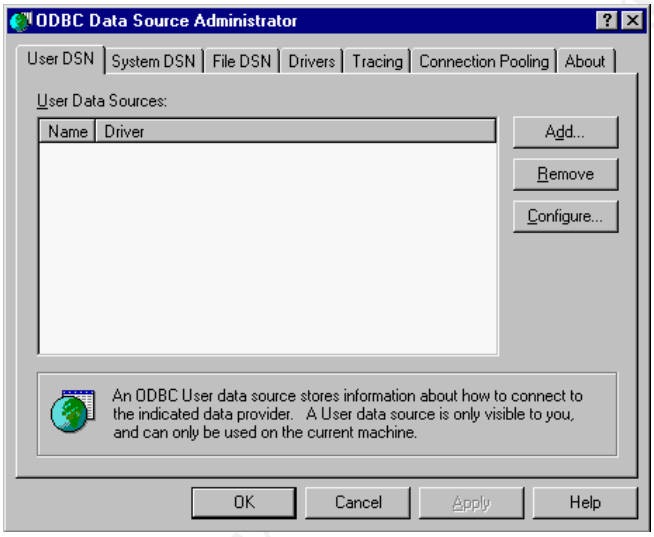
- If the drivers or samples link to the inside, vulnerabilities could exist for an attacker.

Best Practices

- Remove all unused and sample data sources (User, System, and File) from the ODBC Data Source Administrator.
- Remove all unused drivers from the ODBC Data Source Administrator.

Audit

- Open the Control Panel | ODBC Data Source Administrator and check for above practices. See diagram below.



Results

- [ ] All unused data sources and drivers are removed as per policy. Make note of any data sources that are used and explain why.

Notes _____

_____

_____

DISABLE NON-REQUIRED SERVICES

Description

- By default a number of services are installed and active on an NT server that are not required by a web server. To reduce the exposure that could occur due to these services running, they should be disabled.

Risks

- Potential security holes a hacker could exploit in many services.

Best Practices

- The following services should be disabled. Since the web server does not require them.
  - Alerter
  - Clipbook Server
  - Computer Browser
  - DHCP Client
  - Messenger
  - NetBIOS Interface
  - NetLogon
  - Network DDE and Network DDE DSDM
  - Network Monitor Agent
  - NWLink NetBios
  - RPC Locator
  - Server (Only enabled when using User Manager)
  - Simple TCP/IP Service
  - SMTP
  - Spooler
  - TCP/IP NetBios Helper
  - WINS Client (TCP/IP)
- Refer to Microsoft Knowledge Base article Q189271 for more information.

Audit

- Use the Services Manager from the Control Panel to check the above services.

Results

☐ All non-used services are disabled as per policy. If any service listed above needs to be used make note of it and why below.

Notes _____

_____

_____

DISABLE IP ADDRESS IN CONTENT LOCATION

Description

- When a static non-ASP page is retrieved from an IIS server, the URL to the page is given with the IP address of the server. With the server protected by Network Address Translation (NAT) this would reveal the address.

Risks

- The address of the web server, even if protected by NAT, would be shown.

Best Practices

- Disable the use of IP addresses in Content-Location for all file extensions by executing the following command where the file Adsutil.vbs is found:
  - `Cscript.exe adsutil.vbs w3svc/UseHostName True`
- See Microsoft Knowledge Base article Q218180 for more information.

Audit

- Use the Metabase editor from the IIS Resource Kit called METAEDIT.EXE to look for the item `/LM/W3SVC/UseHostName`, the value should be 1.

Results

☐ Disable IP Address in Content Location as per policy.

Notes _____

_____

_____

ADD SYN FLOOD PROTECTION

Description

- The common Denial of Service attack (DoS) is the "SYN Flood". A SYN Flood occurs when thousands of TCP session request packets are sent to a target. The target will replay with a SYN-ACK packet at 3,6,12,24, and 48 second intervals to try and establish a session connection with the source. It will also wait an additional 96 seconds after the last attempt. For each connection request the target NT machine sets asides memory and uses CPU cycles. Each connection request last for a total of 189 seconds. With thousands of connection requests, a DoS occurs.

Risks

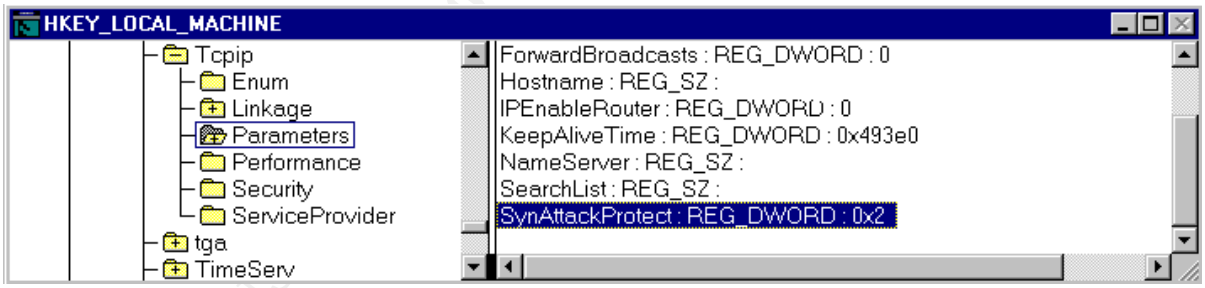
- Large number of DoS attacks bringing down the Web service.

Best Practices

- Set the following registry value to mitigate the damage caused by SYN attacks.
- Change the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect value to 2 (0 is default).
- See Microsoft Knowledge Base article number Q142641 for more information.

Audit

- Use REGEDIT.EXE to look for the value of 2 in the above key. See diagram below.



Results

SynAttackProtect is set to 2 as per policy.

Notes _____

_____

_____

RESTRICT ANONYMOUS NETWORK ACCESS

Description

- An anonymous network access or null user session is a session established over the network with a blank username and blank password. Windows NT allows null user session to remotely download a complete list of usernames, groups and sharenames.

Risks

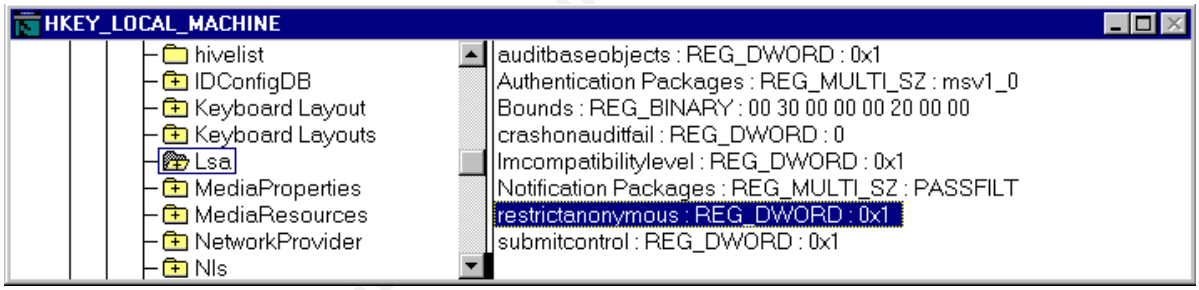
- An attacker could use the null user session to get a list of usernames, group and sharenames and use this information to gain further access to the system.

Best Practices

- Do not allow null user sessions. Set the following registry key to disable.
  - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\RestrictAnonymous set value to a 1.

Audit

- Use REGEDIT to check registry value as per above setting. See diagram below.



Results

☐ Restrict anonymous network access as per policy.

Notes _____

_____

_____

REMOVE REMOTE DATA SERVICE (RDS) SUPPORT

Description

- Part of the Option Pack includes Remote Data Service (RDS). This should not be installed because of know security holes in this service.

Risks

- Attackers could possibly execute arbitrary commands to access other OLE-enabled database servers.

Best Practices

- Do not install the RDS from the Data Access Components in the Option Pack.
- Also remove the following registry keys:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory.
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory.
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\VbBusObj.VbBusObjCls.
- See Microsoft Knowledge Base article number Q184375 for more information.

Audit

- Use REGEDIT.EXE to search for the above keys.

Results

☐ RDS Support has been removed as per policy.

Notes _____

_____

_____

SHUT OFF NTFS 8.3 NAME GENERATION

Description

- NTFS can auto-generate 8.3 names for backward compatibility with 16-bit applications. That means by default NT creates two names for every file.

Risks

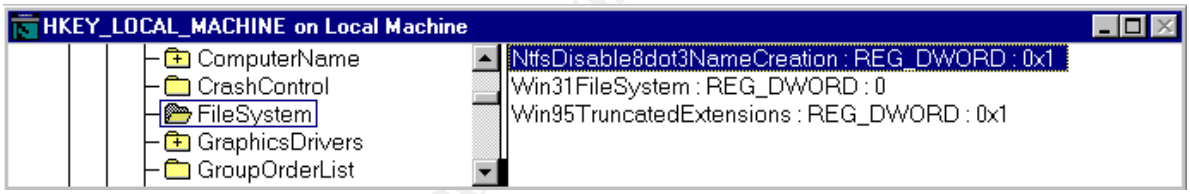
- 16-bit apps pose a security threat and should not be used on a secure web server.

Best Practices

- Turn off 8.3 name generation as shown.
  - Set `NtfsDisable8dot3NameCreation` found in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\` to a 1.
- *Warning* – Disabling 8.3 names may cause poorly written or short name dependent Win32 applications to fail. Test first!

Audit

- Use REGEDIT.EXE to check for value above. See diagram below.



Results

☐ 8.3 Name Generation has been disabled. If this is not possible, make note of why it can not be set below.

Notes _____

_____

_____

Remove Shutdown Button from Logon Dialog

Description

- The Shutdown button is visible be default on Windows NT Logon Dialog Box.

Risks

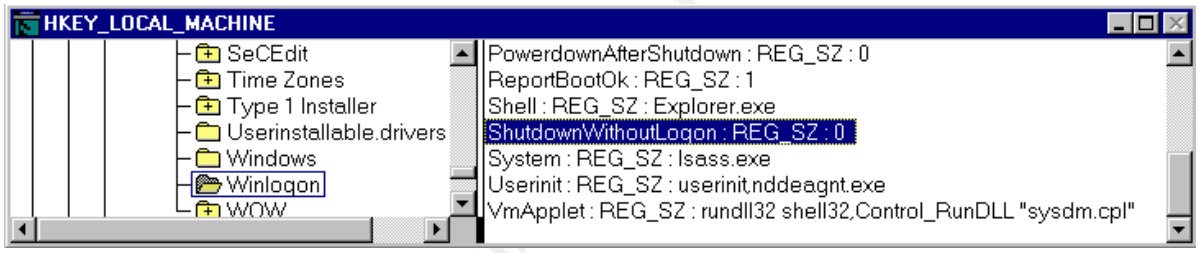
- Users with physical access to server can shut it down with out logging in.

Best Practices

- Remove the Shutdown button from the Windows NT Logon Dialog Box by changing the HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\Windows NT\Current Version\Winlogon\ShutdownWithoutLogon registry value to a 0.

Audit

- Use REGEDIT to check registry value as per above setting. See diagram below.



Results

Shutdown button is off as per policy.

Notes _____

_____

_____

CLEAR PAGING FILE AT SYSTEM SHUTDOWN

Description

- Windows NT by default will not clear the page file at shutdown, thus allowing the next user the possibility of accessing the page file data.

Risks

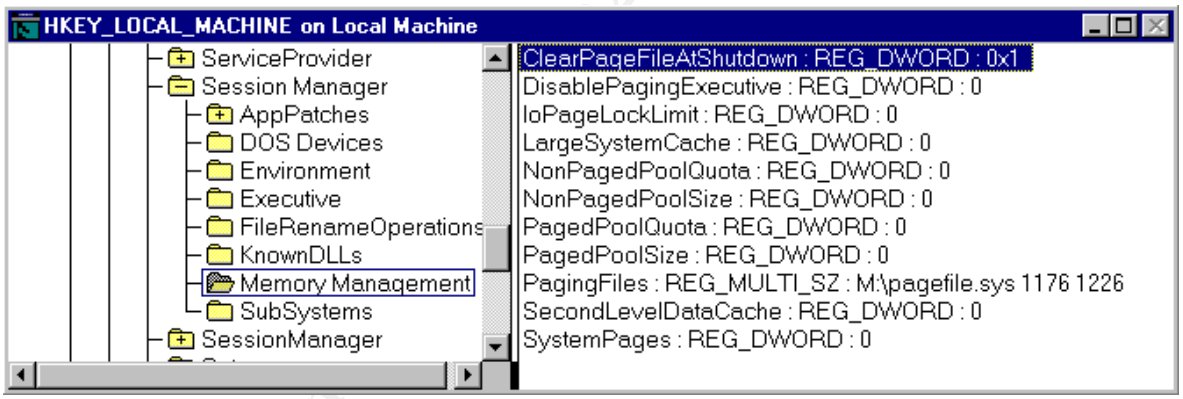
- An attacker could potentially access the page file after installing a Trojan Horse on the system and then forcing a shutdown or crash to occur. Once restarted the page file could be retrieved.

Best Practices

- Clear the page file at system shutdown. Set the following registry key as follows:
  - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown set value to a 1.

Audit

- Use REGEDIT to check registry value as per above setting. See diagram below.



Results

Clear page file at shutdown is on as per policy.

Notes _____

_____

_____

AVOID THE NETWARE DLL TROJAN HORSE

Description

- The Local Security Authority in Windows NT uses a DLL to collect passwords for further authentication on a Netware server. This DLL is not installed in an NT server installation, but the system will try to look for it.

Risks

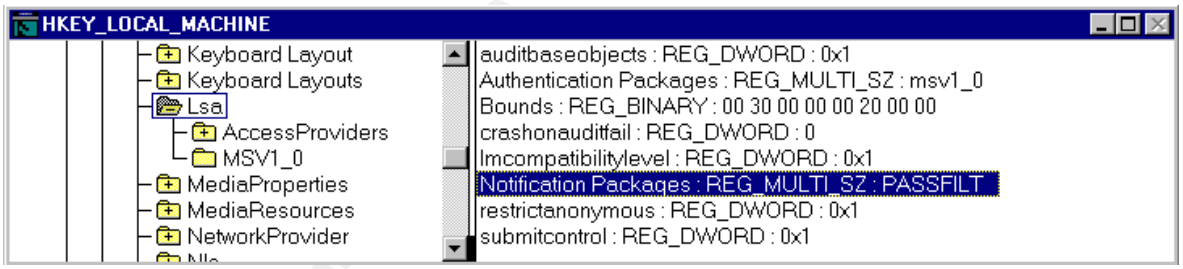
- Users or attackers with write access to %systemroot%/system32 can install a Trojan DLL and collect passwords.

Best Practices

- Since this DLL is only necessary if the MS Netware client is being used, remove the call to it in the registry.
- Remove the entry FPNWCLNT from the following Notification Package.
  - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\Notification Packages.
  - *Warning*: Do not remove any other entry, such as PASSFILT.

Audit

- Use REGEDIT to check registry value as per above setting. See diagram below.



Results

The FPNWCLNT notification package is removed as per policy.

Notes _____

_____

_____

RESTRICT FLOPPY DRIVE AND CD-ROM DRIVE ACCESS TO INTERACTIVE ONLY

Description

- Only the currently logged-on user should be able to access floppy disk drives and CD-ROM drives.

Risks

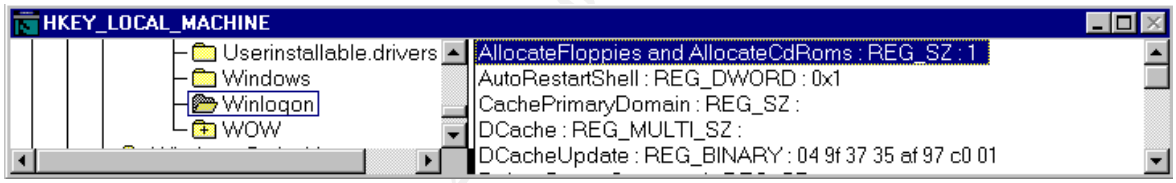
- If not set, then an attacker could access the floppy drive or CD-ROM.

Best Practices

- Restrict floppy and CD-ROM drive access to the logged-on user.
- Change the "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies and AllocateCdRoms" registry value to a "1".
- If the above entry does not exist, or is set to any other value, floppy devices will be available for shared use by all processes on the system.

Audit

- Use REGEDIT to check registry value as per above setting. See diagram below.



Results

Floppy Drive and CD-ROM Drive are restricted to the logged-on user as per policy.

Notes _____

_____

_____

Conclusion

Following the best practices throughout this document, an administrator can attain a certain comfort level with regards to the level of security. By staying on top of the latest security developments and patches the comfort level can remain.

It is extremely important to keep the Security Policy up to date and revise this audit document when any changes or additions occur to the security practices within this document.

Credits and References

- SANS Institute. "Windows NT Security: Step by Step." The SANS Institute, Version 3.03 February 2001.
- Fossen, Jason. "Securing Windows NT Step by Step." The SANS Institute, June 24, 2000.
- Fossen, Jason. "Securing Internet Information Server 5.0." The SANS Institute, February 1, 2001.
- Sutton, Steve. "Windows NT Security Guidelines, Considerations and Guidelines for Securely Configuring Windows NT in Multiple Environments." A Study for NSA Research. Trusted Systems Service, Inc., June 3, 1999.
- Howard, Michael. "Microsoft Internet Information Server 4.0 Security Checklist." Microsoft Corp., March 15, 2001.
- Microsoft Corp. "Windows NT C2 Configuration Checklist." Microsoft Corp., April 5, 2000.
- Microsoft Corp. "Windows NT 4.0 Member Server Configuration Checklist." Microsoft Corp., June 6, 2000.
- "How to Obtain the Latest Windows NT 4.0 Service pack." Microsoft Knowledge Base Article ID: Q152734.
- "Windows NT System Key Permits Strong Encryption of the SAM." Microsoft Knowledge Base Article ID: Q143475.
- "PRB: Security Implications of RDS 1.5, IIS 3.0 or 4.0, and ODBC." Microsoft Knowledge Base Article ID: Q184375.
- "Internet Information Server Returns IP Address in HTTP Header (Content-Location)." Microsoft Knowledge Base Article ID: Q218180.
- "List of Services Needed to Run a Secure IIS Computer." Microsoft Knowledge Base Article ID: Q189271.
- "Internet Server Unavailable Because of Malicious SYN Attacks." Microsoft Knowledge Base Article ID: Q142641.

- Heckendorn, Sherri. SANS GCNT paper (untitled). SANS GIAC Web Site, 2001.
  - Thanks Sherri. I incorporated Sherri's audit format and added my own twist to the layout. I broke apart the testwork section into an audit and results section and separated each category onto it's own page for ease of use.

- Farrington, Dean. SANS GCNT paper "Windows NT Web Server Auditing". SANS GIAC Web Site, 2001.
  - Thanks Dean. I used Dean's idea of auditing a Web Server and expanded on the number of categories to suit my own site's audit requirements and my experiences.

- D'Souza, Clyde. SANS GCNT paper "Developments in NT Auditing". SANS GIAC Web Site, 2001.
  - Thanks Clyde. I included Clyde's design of allowing the auditors to present their findings and expand upon them by writing notes on those results. I expanded on the idea by giving the auditors a lead in statement and giving them the room to give a detail explanation.

- Do, George. SANS GCNT paper "A Brief View into Auditing Windows NT". SANS GIAC Web Site, 2001.
  - Thanks George. I expanded on George's 'Service Packs' section and included Hot Fixes, since Microsoft infrequently rolls out service packs, but creates Hot fixes for all known vulnerabilities soon after they are found and reported. It is also critical to stay up to date on vulnerability news at sites such as www.sans.org or www.windowsitsecurity.com to get the latest information.

- Shawgo, Jeff. SANS GCNT paper "Consolidated Security Event Monitoring for Microsoft Windows NT 4.0 Server". SANS GIAG Web Site, 2001.
  - Thanks Jeff. I used Jeff's detailed document and expanded on the auditing portion to describe to the auditors using this report; how to check for proper Windows NT audit settings. It was realized that this was out side of Jeff's document scope.