Securing NT Server 4.0

How to implement a secure NT server

Allaire Security White Papers Series

(Version 1.0)

Abstract

Title	Securing NT Server 4.0
Last Tech. Update	June 29, 2000
Product	Microsoft NT Server 4.0
Target Audience	Network and System Administrators
Abstract	Securing an NT server can be a difficult process, considering the dizzying number of security advisories administrators must keep track of. This is Allaire's effort toward making that job a little easier. While we recommend that organizations consider many of the techniques described here, we also recommend that each organization perform its own testing when developing an NT lock-down strategy.

Allaire Corporation • One Riverside Center • 275 Grove Street • Newton • MA • 02466
www.allaire.com • info@allaire.com • (617) 219-2000 •
security issues: secure@allaire.com
document feedback: lockdown@neohapsis.com

Table of Contents

Securing Windows NT Server 4.0 Overview

This document provides information on securely implementing and locking-down Microsoft Windows NT Server 4.0-based systems. We assume the reader is already familiar with the NT 4.0 installation process, configuration process and general system administration tasks.

We will discuss, in detail, the five steps necessary for securely deploying Windows NT Server 4.0 in a web and e-commerce environment. Briefly, the five steps are:

1. Installing NT Server and applying Service Pack 6a
2. Applying any necessary hotfixes
3. Addressing the issues discussed in a number of Microsoft Security Bulletins
4. Disabling unused services and subsystems
5. Making registry modifications

Organizations should strongly consider all included suggestions. However, it is important for organizations to create a *tested* solution for their individual needs, and form a standardization effort around their results. Creating a unified and documented approach for deploying NT securely is achievable with planning. Unfortunately, the same breadth of features that allow Windows NT Server to be as versatile as it is also makes it hard to properly secure. This diversity prevents dictating a universal method of secure configuration. Instead, this document seeks to make a number of strong suggestions.

Finally, this document provides a number of external resources and tools for further NT Server 4.0 configuration and monitoring. See Appendix B “Resources and Tools” for further information.

Assumptions

Because there is no “one size fits all” strategy for deploying Windows NT securely, this document makes the following assumptions:

1. **Window NT 4.0 Server with Service Pack 6a applied**. This document assumes the reader has or will apply Service Pack 6a.. It fixes a *wide array* of Windows NT security problems (find a complete list of bug fixes at: http://support.microsoft.com/support/kb/articles/q241/2/11.asp). Without Service Pack 6a, many of the configuration options discussed are not applicable. Please be sure to note that the initial Service Pack 6 (as opposed to 6a) contained a regression

error—make sure you have the updated version (6a).

2. **The Windows NT Servers will be used for web-based environments**. While many of the techniques detailed here apply to servers being used for simple file-and-print sharing, the focus of this document is on securing NT servers used for web-based services.

3. **Physical security is assumed**. The recommendations in this document assume that the organization's servers have been physically secured. Without physical security, there is little hope of maintaining a secure operating environment.

4. **Only system administrators will perform local logins**. While it is possible for users to login locally to Windows NT servers, we assume that only admin-level users will be logging into the machines locally.

5. **Further configuration changes specific to the web-server being used (MS IIS, SUN-Netscape iPlanet, etc.) will be necessary**. Please see the Allaire Security White Paper: Securing IIS document.

Installation considerations and Service Pack 6a

If you're fortunate enough to be installing NT 4.0 from scratch, we have a few initial recommendations:

1. Consider using the Custom Install option—this lets you choose only those options required to run your system. However, even this install may result in a number of unnecessary services and protocols that should be shut down or removed. We suggest the following installation considerations:

    - If presented with the option, do *not* install Internet Information Server (IIS) versions 2.0 or 3.0. Doing so may introduce additional security vulnerabilities. Instead, install only the version you intend to run. (IIS note: IIS 4.0 does not typically ship with Windows NT installs—it can be found in the Windows NT Option Pack).
    - If your server will act only as an Internet web server, uncheck IPX and NetBEUI in the 'Network Protocols' setup window.
    - When you reach the 'Network Services' setup window, only add strictly required services. No additional services are needed for a TCP/IP-based Internet web server.

2. Always use NTFS disk partitions instead of FAT. NTFS offers security features; FAT does not. If you must use a FAT partition, do not place any system files on it. Also, be careful about putting any sensitive information on that partition - you cannot set

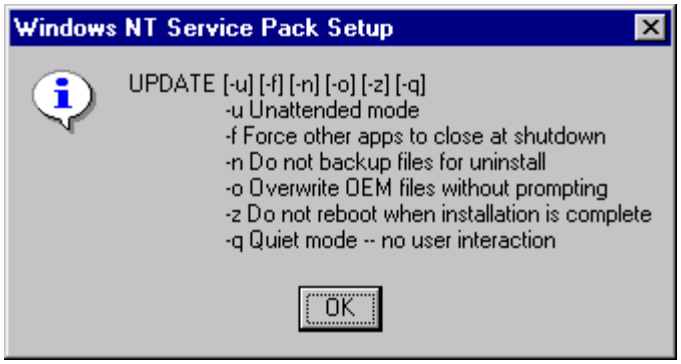
any access permissions for files and directories on FAT partitions. Using FAT for the system partition is *very* unsecure.

3. If your Windows NT system was ever installed on a FAT partition, reinstall it from scratch. Converting a current FAT-based system partition to NTFS after the installation process will not sufficiently set file permissions. Remember, FAT will not help in the long run when it comes to NT.

Service Pack 6a
Microsoft releases a collection of recommended fixes in a bundle referred to as a 'Service Pack.' The latest service packs can be found at
http://www.microsoft.com/downloads/search.asp

Note: *Use the "Keyword Search" option at the top of the screen and search for "sp6."*

Display the following dialog box by running "*Update.exe* /?", where *Update.exe* is any support pack or hot fix file you wish to execute. Be aware, the dialog box is not displayed until after it finishes extracting the files. These option switches can be helpful when used with SMS or any other distribution tool for distributing the update to client machines. Options are not a requirement and the service pack can be installed without them.



For a list of the fixes included in Service Pack 6a please refer to:
http://support.microsoft.com/support/kb/articles/q241/2/11.asp

Installing Hotfixes

Hotfixes are security patches released by Microsoft to fix specific, post-service pack problems. Some hotfixes may be security-related, but most are more operational fixes. While it may be tempting to install every released hotfix, Microsoft encourages hotfix

installations only on an “as-needed” basis. The following is an excerpt form Microsoft’s KB article Q246467 detailing the “pppcon” hotfix:

> A supported fix that corrects this problem is now available from Microsoft, but it has not been fully regression tested and should be applied only to computers that are experiencing this specific problem. If you are not severely affected by this specific problem, Microsoft recommends that you wait for the next Windows NT 4.0 service pack that contains this fix.

Source: Microsoft Knowledge Base Article: RAS Server Stops Responding to New PPP Connection Requests (Q246467) [online]. [Redmond, Washington, USA] : Microsoft, November 2000 [cited 5 January, 2001]. Available from World Wide Web: < http://support.microsoft.com/support/kb/articles/Q246/4/67.ASP >.

The hotifx rule-of-thumb is: if you don’t absolutely need it don’t apply it. Hotfixes are not regression tested and can cause strange problems. However, there have been security problems that were so damaging that administrators chose to apply the hotfix anyway since – the security risk was greater than regression concerns.

Fortunately, at the time of this writing the only security-related hotfix post Service Pack 6a is the “C2-Fix. You can find out more about this fix by reading the Microsoft Knowledge Base Article Q244599, which you can find at http://support.microsoft.com/support/kb/articles/Q244/5/99.ASP.

Organizations concerned about following “C2” guidelines might be interested in this particular patch, but most organizations need not worry about it. (For more information on C2 see the document “C2 Administrator’s and User’s Security Guide Revision 1.1” at http://www.microsoft.com/technet/security/c2eval.asp.

Administrators should keep an eye on both the Windows NT Security Bulletins (go to http://www.microsoft.com/technet/security/current.asp and search by product), as well as Microsoft’s hotfix ftp site at: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postsp6a/.

Addressing Microsoft Security Bulletins

Microsoft addresses vulnerability concerns by releasing security bulletins and associated patches. Please note that some patches are not available as hotfixes or not found in the typical update locations—therefore it’s important that you monitor Microsoft’s site (and/or subscribe to its notification service at http://www.microsoft.com/technet/security/notify.asp) for new bulletin alerts.

Apply all patches that are pertinent to the services you run. The chart below lists, in order of their release date, available security patches at the time this document was last

updated. The ‘Affected Component’ column lists the particular NT service or component affected. All patches labeled 'Core NT,' as well as patches pertaining to any installed services (such as IIS, MS SQL Server, Print Services, etc.) must be applied. The ‘Remote’ column states whether or not a patch affects vulnerabilities that can be executed remotely. Be sure to take up the task of analyzing more recent Microsoft Security Bulletins where this chart leaves off.

Patch by Month	Release Date	Affected Component	Remote
MS99-047: Patch Available for "Malformed Spooler Request" Vulnerability	11/4/1999	Print Services	Y
MS99-048: Patch Available for "Active Setup Control" Vulnerability	11/11/1999	Internet Explorer	N
MS99-051: Patch Available for "IE Task Scheduler" Vulnerability	11/29/1999	Core NT/Internet Explorer	N
MS99-054: Patch Available for "WPAD Spoofing" Vulnerability	12/1/1999	Internet Explorer	N
MS99-053: Patch Available for "Windows Multithreaded SSL ISAPI Filter" Vulnerability	12/2/1999	IIS	Y
MS99-050: Patch Available for "Server-side Page Reference Redirect" Vulnerability	12/8/1999	IIS	Y
MS99-055: Patch Available for "Malformed Resource Enumeration Argument" Vulnerability	12/9/1999	Core NT	Y
MS99-056: Patch Available for "Syskey Keystream Reuse" Vulnerability	12/16/1999	Syskey	N
MS99-057: Patch Available for "Malformed Security Identifier Request" Vulnerability	12/16/1999	Core NT	Y
MS99-059: Patch Available for "Malformed TDS Packet Header" Vulnerability	12/20/1999	SQL Server	Y
MS99-058: Patch Available for "Virtual Directory Naming" Vulnerability	12/21/1999	IIS	Y
MS99-061: Patch Available for "Escape Character Parsing" Vulnerability	12/31/1999	IIS	Y
MS00-001: Patch Available for "Malformed IMAP Request" Vulnerability	1/4/2000	MCIS	Y
MS00-003: Patch Available for "Spoofed LPC Port Request" Vulnerability	1/12/2000	Core NT	N
MS00-005: Patch Available for "Malformed RTF Control Word" Vulnerability	1/17/2000	MS Office/MS Write	N
MS00-004: Patch Available for "RDISK Registry Enumeration File" Vulnerability	1/21/2000	Core NT	N

MS00-006: Patch Available for "Malformed Hit-Highlighting Argument" Vulnerability	1/26/2000	IIS	Y
MS00-007: Patch Available for "Recycle Bin Creation" Vulnerability	2/1/2000	Core NT	N
MS00-009: Patch Available for "Image Source Redirect" Vulnerability	2/16/2000	Internet Explorer	N
MS00-010: Patch Available for "Site Wizard Input Validation" Vulnerability	2/18/2000	IIS/SiteServer	Y
MS00-011: Patch Available for "VM File Reading" Vulnerability	2/18/2000	Internet Explorer	N
MS00-012: Patch Available for "Remote Agent Permissions" Vulnerability	2/22/2000	SMS Client	N
MS00-013: Patch Available for "Misordered Windows Media Services Handshake" Vulnerability	2/23/2000	Media Services	Y
MS00-015: Patch Available for "Clip Art Buffer Overrun" Vulnerability	3/6/2000	Internet Explorer/MS Office	N
MS00-014: Patch Available for "SQL Query Abuse" Vulnerability	3/8/2000	SQL Server	Y
MS00-008: Patch Available for "Registry Permissions" Vulnerability	3/9/2000	Core NT	Y
MS00-016: Patch Available for "Malformed Media License Request" Vulnerability	3/17/2000	Media Services	Y
MS00-018: Patch Available for "Chunked Encoding Post" Vulnerability	3/20/2000	IIS	Y
MS00-019: Patch Available for "Virtualized UNC Share" Vulnerability	3/30/2000	IIS	Y
MS00-021: Patch Available for "Malformed TCP/IP Print Request" Vulnerability	3/30/2000	Print Services	Y
MS00-022: Patch Available for "XLM Text Macro" Vulnerability	4/3/2000	Internet Explorer/MS Office	N
MS00-024: Tool Available for "OffloadModExpo Registry Permissions" Vulnerability	4/12/2000	Core NT	N
MS00-023: Patch Available for "Myriad Escaped Characters" Vulnerability	4/12/2000	IIS	Y
MS00-025: Procedure Available to Eliminate "Link View Server-Side Component" Vulnerability	4/17/2000	IIS	Y
MS00-027: Patch Available for "Malformed Environment Variable" Vulnerability	4/20/2000	Core NT	N
MS00-028: Patch Available for "Server-Side Image Map Components" Vulnerability	4/21/2000	IIS	Y
MS00-031: Patch Available for "Undelimited .HTR Request" and "File Fragment Reading via .HTR" Vulnerabilities	5/10/2000	IIS	Y
MS00-030: Patch Available for "Malformed Extension Data in URL" Vulnerability	5/11/2000	IIS	Y
MS00-034: Patch Available for "Office 2000 UA Control" Vulnerability	5/12/2000	Internet Explorer/MS Office	N

MS00-033: Patch Available for "Frame Domain Verification", "Unauthorized Cookie Access", and "Malformed Component Attribute" Vulnerabilities	5/17/2000	Internet Explorer	N
MS00-029: Patch Available for "IP Fragment Reassembly" Vulnerability	5/19/2000	Core NT	Y
MS00-036: Patch Available for "ResetBrowser Frame" and "HostAnnouncement Flooding" Vulnerabilities	5/25/2000	Core NT	Y
MS00-038: Patch Available for "Malformed Windows Media Encoder Request" Vulnerability	5/30/2000	Media Services	Y
MS00-035: Patch Available for "SQL Server 7.0 Service Pack Password" Vulnerability	5/30/2000	SQL Server	N
MS00-037: Patch Available for "HTML Help File Code Execution? " Vulnerability	6/2/2000	Internet Explorer	N
MS00-039: Patch Available for "SSL Certificate Validation" Vulnerabilities	6/5/2000	Internet Explorer	N
MS00-040: Patch Available for "Remote Registry Access Authentication " Vulnerability	6/8/2000	Core NT	Y
MS00-041: Patch Available for "DTS Password" Vulnerability	6/14/2000	SQL Server	Y
MS00-042: Patch Available for "Active Setup Download" Vulnerability	6/29/2000	Internet Explorer	N

Disabling unused services and subsystems

By default, the Windows NT Server 4.0 installation process installs and activates a wide range of frequently unneeded services and subsystems. Most security professionals agree: Only run necessary services and subsystems. Disabling unneeded or unused services greatly reduce potential system vulnerabilities and increase the server's stability. For example, leaving FTP (File Transfer Protocol) enabled--even if you're not using it-- allows potential intruders to gather information about your system and user accounts.

Removing the NetBIOS Interface Service

Many administrators remove the NetBIOS interface bindings. While this undoubtedly adds a level of security, it can also cripple a number of Microsoft applications and/or Windows functionality that rely on NetBIOS-based communications. For example, you won't be able to remotely administrate the NT Server via the various included management tools (MMC, User Manager, Server Manager, etc).

If you must use NetBIOS for administration, any Internet-attached NT server should be placed behind a network-access-control device such as, a firewall or packet filtering router. In addition, access of ports 135-139 (used by NetBIOS) should be restricted to the internal interface only. If you're running a simple web-server that does not require NetBIOS, remove the binding entirely—you can always administer the IIS web service over HTTP via the administrative virtual server that is placed on a high port.

To Disable NetBIOS Service on a “per NIC” basis:

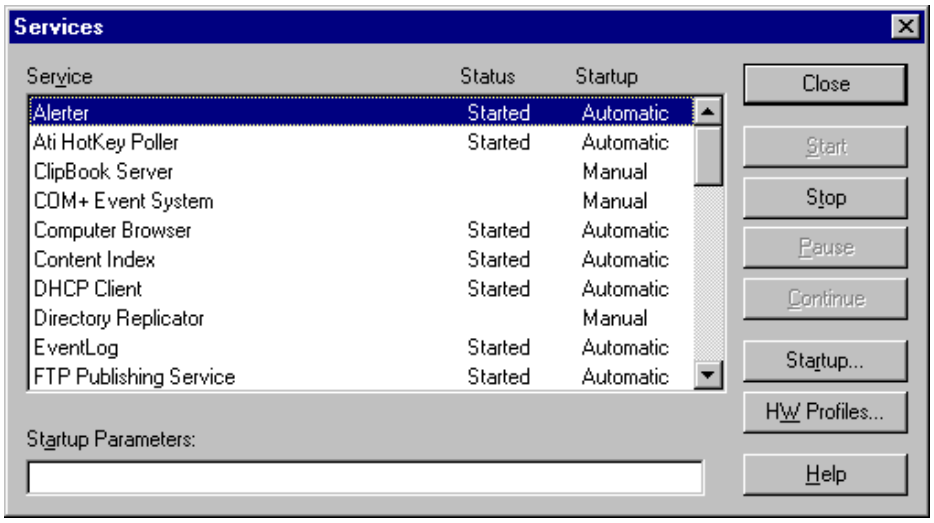
1. Right click on Network Neighborhood
2. Click on Properties
3. Click on Bindings Tab
4. Select “All Services” from the drop-down “Show bindings for” dialog box
5. Expand the NetBIOS Service list
6. Select the appropriate network adapter card
7. Press Disable

To Remove the NetBIOS protocol completely (all NICs):

1. Open the Services Applet from within the Control Panel
2. Click on NetBIOS
3. Click on Remove

Services started on boot

The system should always start with the least amount of necessary services possible. Service initialization is controlled in the Services Applet to the Windows NT Control Panel as illustrated below:



Below is a list of commonly installed services. Be assured that this list varies from machine to machine. The best way to make sure you’re safe is to verify each and every one for necessity, and remove those not required.

***NOTE**: There is one important aspect to keep in mind when dealing with the SNMP service. As with all other services, if you do not need SNMP, turn it off. If you do need SNMP, make sure you change the community string to something besides the default.*

Service	Required	Purpose
Alerter	N	Lets a user receive messages from other machines
Clipbook Server	N	Lets clipboard be shared over network
Computer Browser	Y	A service for gathering and distributing resource information throughout the network
DHCP Client	N	Enables machine to receive network addresses information via DHCP (Dynamic Host Configuration Protocol)
Directory Replicator	N	Lets NT import and export directory contents to and from other systems
Microsoft DNS Server	N**	Lets server act as a DNS Server
Event Log	Y	Allows for system logging
FTP	N***	FTP service is for transferring incoming and outgoing files
Gopher	N	Gopher is an old protocol prior to HTTP (web); provided by Internet Information Server 3.0.
License Logging	N	Relies on NetBIOS over IP; this is similar to the Alerter Service
Net Logon	Y	Used by Server and Workstation; it provides for network Authentication
Network DDE and DDE DSDM	N	Used for Dynamic Data Exchange and applications requiring this functionality. Chat is a good example of an application requiring DDE
Network Monitor Agent	N	Used to monitor traffic passing through NICs
NT LM Security Support Provider	Y	Helps with backward compatibility for older software packages
Plug and Play	N	Used to configure PNP devices
Remote Procedure Call Locator and Services	Y	Maintains and services requests for applications on servers using RPC
Routing and Remote Access Service (RRAS)	N	Enhancement to remote access services
Schedule	N	Lets applications be executed at predesignated times.
Server	Y*	Used for all NetBIOS applications. Server Manager and other administrative tools require this service
Simple TCP	N	Implements various classic diagnostic and utility services
SNMP	N	Simple Network Management Protocol allows for remote monitoring of the server
Spooler	N	Lets server accept print for spooling to network or local printers
TCP/IP NetBIOS Helper	Y*	Used to enhance NBT and assist Net Logon service
Telephony	N	Used to manage telephony drivers and dialing properties
UPS	N	Used to manage serial communications with a UPS (Uninterruptable Power Supply)
WINS	N	Lets system act as a Windows Internet Name Server
World Wide Web Publishing Service	Y	Web server provided by Internet Information Server
Workstation	Y*	Allows for outbound NetBIOS connections. This is part of the core services NT 4.0 requires to run a webserver.

* Required for administration/access to the system via NetBIOS.
** You may need to enable the DNS service if you do not have a dedicated DNS server.

*** While FTP is not required, you will need a method to transfer updated web files to the server. If you do not use NetBIOS, or need to transfer files via the Internet, you'll need to enable the service.

Locking down the registry, the file systems and the user rights

There are many security considerations surrounding the NT registry. Administrators can modify the registry using one of two applications: "regedit" and "regedt32." We suggest using *regedt32* for making recommended changes.

Specific registry and files-system modifications are listed in Appendix A. These changes are categorized as follows:

Recommended registry modifications
The registry contains most of the Windows NT initialization and configuration information. Potential security threats include: remote access to the registry, remote enumeration of domain and server configurations, insecure data communication, insecure access via local console logon and insecure access for user-level applications to devices or other system resources.

There are significantly more configuration changes to be made when securing an NT server against local access threats. Since the assumption of physical security has been made, these items are identified as *low* priority. Changes to secure a remotely accessed server or other important security modifications are identified with *high* or *med(ium)* importance.

Protecting the registry itself
The registry, like the file system, contains ACL (Access Control List) information that can be used to limit access to specific Hives, Keys and Sub-Keys. While NT, by default, provides a minimum level of access control, there are several changes needed to limit access to users, groups and/or applications that might try to read and/or modify registry information. Because many applications require access to specific keys in the registry, it is very important to test aspects of all applications running on your system that might need specific access to the registry.

As with the registry values, the registry ACL modifications are prioritized according to importance. Permissions that effect remote access fall into the *high* and *med* categories, while permissions effecting local user or application access are identified as *low*.

Changing default file permissions
During installation, Windows NT makes default ACL changes to the file system. This is assuming you choose an NTFS partition to install your boot partition. During a standard installation, these configuration changes are applied after the system files are installed.

These *do not* get applied during a conversion from FAT to NTFS, (i.e. when using the *convert* utility). These modifications make changes to the system directory (\WINNT by default), and should be modified according to Appendix A. Most of these changes effect local console or application access to critical system files and carry either *med* or *low* importance. The one exception is the Repair directory, which includes backup copies of your computer security database--this is identified as having *high* importance. Every time you make an ERD (Emergency Repair Disk), NT 4.0 makes a copy of the SAM (Security Accounts Manager) and places it in the Repair directory. Be aware that many security vulnerabilities effecting local user or application access can also be remote vulnerabilities if your server is not properly secured against remote compromise.

Changing default user rights
Appendix A identifies only one change to the default user rights on NT Server. This right controls who can access the server from the network. By default, NT server allows *everyone* to access the server from the network. Change this to *Users* (or your appropriate group for network access to the server).

Other security considerations

The following are additional steps for securing NT 4.0.

Note: *Not all of these suggestions apply to all environments – they should be evaluated on an option-by-option basis*.

Removing the OS/2 and POSIX subsystems:
Windows NT only supports OS/2 1.x text-mode applications and POSIX 1.0 applications in text mode. If these subsystems are not required, remove them. This is covered as part of the registry changes listed in Appendix A.

The use of passfilt
The passfilt.dll utility was introduced with service pack 2 and can be used to help prevent poor or "weak" passwords by requiring passwords of at least six characters and a combination of three of the following: uppercase, lowercase, numbers or characters. Weak passwords have traditionally accounted for a large number of security breaches in years past – this utility can be used to curb that trend. See KB article Q161990 at http://support.microsoft.com/support/kb/articles/Q161/9/90.asp

The use of passprop
Similar to passfilt.dll, passprop.exe is also used to enforce stronger passwords. It's found in the NT Resource Kit /i386/NETADMIN. It provides four switches for setting various security features:

/simple – Windows default
/complex – Requires a mix of uppercase, lowercase, numbers or characters

/adminlockout – Allows admin lockout except under certain conditions
/noadminlockout – Does not allow admin to be locked out (Windows default)

SMB Signing
SMB (Server Message Block) authentication protocol is also known as the CIFS (Common Internet File System). SMB signing requires every packet be signed and verified. You may see a decrease in performance of up to 10 or 15 percent when implementing SMB. See KB Q161372 found at
http://support.microsoft.com/support/kb/articles/Q161/3/72.asp

Kill LM authentication if LM Auth is unnecessary
LM, or LanManager authentication, is a weaker form of Authentication included in NT for compatibility with older products. Prior to service pack 4, NT always used both LM authentication, as well as its own NTLM authentication. Since LM authentication is a weaker authentication model, disable it. See KB Q147706 found at
http://support.microsoft.com/support/kb/articles/Q147/7/06.asp

Use of Syskey
Since the SAM database stores password hashes for domain and local computer accounts, a password-cracking tool can be used to gain access to the passwords stored in the SAM. Syskey encrypts the SAM database with a stronger encryption technique. See KB Q143475 found at
http://support.microsoft.com/support/kb/articles/Q143/4/75.asp

Use of SCM
Security Configuration Manager is designed to provide a central repository for security-related administrative tasks. Security Configuration lets you configure and analyze security on one or more Windows NT machines in your network. For more information see http://www.microsoft.com/TechNet/winnt/Winntas/technote/scmnt4.asp.

Logging Concerns
There are many considerations when configuring Windows NT event logs. One of the primary concerns is that the event logger is granted enough space. To configure the maximum log size, launch the event viewer and choose “Log Settings” under the “Log” pull-down menu. In addition to size, be aware of how logging is handled in the event that the logs are filled. While overwriting logs is never desirable, many prefer this to the alternative of ending the logging cycle entirely. Another alternative is to develop a cycle of backing-up the logs and starting a new one on a regular basis.

You may wish to centralize your logging efforts by outputting all event logs to a centralized logging server. This is accomplished by using the basic NT event logging service, or by using third-party syslog utilities. See Appendix B for more information on logging tools.

Finally, the most important part of logging is reviewing the logs. Become familiar with this critical function of NT 4. What good is a log if no one ever looks at it?

Summary

Since the NT environment is so dynamic, testing these changes before putting them into production is *critical*. Each system is unique and may need to be secured in a different manner. Be aware of what you need to achieve and develop security based on that objective.

New vulnerabilities are uncovered daily, so it's important to keep informed of both potential vulnerabilities and their available fixes. To maintain awareness, subscribe to Bugtraq or the SANS weekly vulnerability list as well as monitoring Microsoft's site for new security bulletins (or subscribe to the service). See Appendix B for URLs for these sites.

Appendix A - Modification Tables

Registry Modifications

There are several registry keys, values and permissions-issues to carefully consider for your environment. Make all suggested changes unless they will cause known issues in your environment. However, just as making any other security related modifications to your system we advise completing one or more standard builds for your environment and complete extensive testing on the final builds to insure that no adverse effects will occur on your production hosts.

Issues listed below are split into editing changes and permissions modifications and have been assigned a level of importance (Low, Med, High), based on a perceived level of threat to your host and the potential level of compromise that might occur.

Item	Purpose	Priority	Changes
Registry Edits			
Clear last logon name from console	Prevents the last successfully logged-on user name from appearing in a new logon request box.	High	Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows NT\CurrentVersion\ Winlogon\ Add Value: DontDisplayLastUserName Data Type: REG_SZ String: 1
Remove Shut-down button from logon dialogue	Prevents users from shutting-down the system prior to local console logon.	High	Key: HKEY_LOCAL_MACHINE\SOFTWARE \ Microsoft\Windows NT\Current Version\ Winlogon\ Add Value: ShutdownWithoutLogon Data Type REG_SZ String: 0
Restrict anonymous access to public LSA (Local Security Authority) information	Restricts anonymous access to LSA. The LSA handles aspects of security administration on the local computer, including access and permissions. This setting restricts anonymous connections (null sessions) from retrieving host enumeration information (user lists, share names, trust information, etc). However, this may also prevent administrators from retrieving user information across different NT Domains under certain circumstances. See MS KB Q143474 for more information.	High	Key: HKEY_LOCAL_MACHINE\SYSTEM \ CurrentControlSet\Control\LSA\ Add Value: RestrictAnonymous Data Type REG_DWORD Value: 1
Restrict null session access over named pipes	Restricts unauthorized access over the network using null sessions over named pipes.	High	Key: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\LanmanServer\ Parameters\ Remove Value: NullSessionPipes Remove Value: NullSessionShares

Item	Purpose	Priority	Changes
Restrict the use of LM authentication	Restricts the use of LM authentication over the network. LM authentication uses a less secure form of encryption. By default, NT uses both LM and NTLM challenge/response when authenticating. You may enforce various scenarios which may restrict the use of LM to "never" (Windows for WG and Win95/98 must use this), or "only when required by the client."	High	Key: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\LSA\ Add Value: LMCompatibilityLevel Type: REG_DWORD Value: 0-5 (Default 0) Level 0 – Send LM response and NTLM response; never use NTLMv2 session security Level 1 – Use NTLMv2 session security if negotiated Level 2 – Send NTLM authentication only Level 3 – Send NTLMv2 authentication only Level 4 – DC refuses LM authentication Level 5 – DC refuses LM and NTLM authentication (accepts only NTLMv2)
Enable secure file sharing (SMB)	Enables and requires SMB message signing. When enabled, SMB authentication uses mutual authentication and message authentication. By default, workstations are enabled once SP-3 is installed, however, servers are not. This will cause a performance degradation to your system. It may also cause client denials in some circumstances, if it has been enabled *and* required by the server, but is not enabled on a client.	Med	Key: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\LanManServer\ Parameters Value: EnableSecuritySignature Type: REG_DWORD Value: 1 Key: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\LanManServer\ Parameters Value: RequireSecuritySignature Type: REG_DWORD Value: 1
Secure base objects	Configures Session Manager for high level of security on these objects. Prevents users from obtaining local administrator access through the use of a DLL. See MS Security Bulletin 99-006 for more info.	Med	Key: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Session Manager Add Value: ProtectionMode Type: REG_DWORD Value: 1
Disable local logon profile caching	Disables the local profile cache. If a logon profile is cached and a domain controller cannot be found, an authorized user can logon to a machine even if the user's domain account has been disabled.	Med	Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows NT\CurrentVersion\ Winlogon\ Add Value: CachedLogonsCount Type: REG_SZ String: 0
Set the page file to be removed at shutdown	Clears the page-file during normal shutdown. By default, the page-file, which may contain sensitive information, is not cleared during shutdown, thereby, making it potentially accessible.	Med	Key: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\ Session Manager\Memory Management Add Value: ClearPageFileAtShutdown Type: REG_DWORD Value: 1

Item	Purpose	Priority	Changes
Enforce strong user passwords	Forces user passwords to be compared against passfilt.dll which checks for quality against dictionary words, username, length and character types.	Med	Key: HKEY_LOCAL_MACHINE\SYSTEM CurrentControlSet\Control\LSA\ Value: Notification Packages Type: REG_MULTI_SZ Add String: “PASSFILT” (do not remove existing ones).
Restrict anonymous access to Application and System Eventlogs	Restricts ability of unauthorized users from viewing the Application and System Event logs. Guest and anonymous connections should be restricted from this activity. The security log is restricted to those users with the “Manage Audit Logs” user right.	Med	Key: HKEY_LOCAL_MACHINE CurrentControlSet\Services\EventLog\ [LogName]\ Add Value: RestrictGuestAccess Type: REG_DWORD Value: 1 Where [LogName] = Application and/or System
Restrict access to add a new printer	Restricts ability of unauthorized users from installing print devices. This value should be edited to allow only administrators to add new printers on a server.	Med	Key: HKEY_LOCAL_MACHINE\SYSTEM CurrentControlSet\Control\Print\Providers\ LanMan Print Services\Servers\ Add Value: AddPrinterDrivers Type: REG_DWORD Value: 1
Remove FPNWCLNT trojan bug	Disables trojan bug *only* if not using FPNW.	Low	Key: HKEY_LOCAL_MACHINE\SYSTEM CurrentControlSet\Control\LSA\ Value: Notification Packages Type: REG_MULTI_SZ Remove String: “FPNWCLNT” (do not remove any other ones).
Disable CD-ROM drive Autorun	Disables Autorun feature for CD-ROMs that initiate a program when placed in drive.	Low	Key: HKEY_LOCAL_MACHINE\SYSTEM CurrentControlSet\Services\CDrom\ Value: Autorun Type: REG_DWORD Value: 0

Item	Purpose	Priority	Changes
OS/2 and POSIX sub-system support	Removes support for these sub-systems. This support has never been tested in a secure environment. Therefore, unless specific need is required, this support should be removed.	Low	Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\OS/2 Subsystem for NT Delete all sub keys Key: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\ Session Manager\Environment\ Delete Value: Os2LibPath Key: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\ Session Manager\SubSystems\ Delete Value: Optional Key: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\ Session Manager\SubSystems\ Delete Values for Posix and OS/2
Protect kernel object attributes	Restricts the ability of the object manager to change kernel object attributes in the object table for the current process, if and only if the previous mode of the caller is kernel mode.	Low	Key: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Session Manager\ Add Value: EnhancedSecurityLevel Type: REG_DWORD Value: 1
Secure additional base name objects	Applies additional security to several objects not addressed by the "Secure Base Objects" modification, including RotHintTable and ScmCreatedEven.	Low	Key: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Session Manager\ Add Value: AdditionalBaseNamedObjectsProtectionMode Type: REG_DWORD Value: 1
Enable auditing of base objects	Auditing of these objects cannot be enabled through User Manager. If access to these objects is a concern, enable auditing through the registry.	Low	Key: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Lsa\ Add Value: AuditBaseObjects Type: REG_DWORD Value: 1
Enable auditing of backup and restore privileges	Auditing of these privileges cannot be enabled through User Manager. Since users with these privileges can sometimes bypass security policies, it may be a concern to audit these events.	Low	Key: HKEY_LOCAL_MACHINE\SYSTEM\ Key CurrentControlSet\Control\Lsa\ Add Value: FullPrivilegeAuditing Type: REG_BINARY Value: 0x01 (hex)
Enable NetBT to open TCP and UDP ports for exclusive access	Prevents unprivileged user mode applications from listening to TCP and UDP ports used by NT services.	Low	Key: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\NetBT\Parameters\ Add Value: EnablePortLocking Type: REG_DWORD Value: 1

Item	Purpose	Priority	Changes
Restrict access to floppy drive and CD-ROM	Prevents these devices from being accessed by any process except for the currently logged-on user.	Low	Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows NT\CurrentVersion\ Winlogon\ Add Value: AllocateFloppies Add Value: AllocateCdRoms Type: REG_SZ Value: 1
Force shut-down of system when security event log becomes full	Halts the system if the system is prevented from writing to the security log. If the security event log is set to "Do Not overwrite events", you may want to enable this to prevent any period of un-logged activity.	Low	Key: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Lsa\ Add Value: CrashOnAuditFail Type: REG_DWORD Value: 1
Logon Notice	Notify users that unauthorized access is not allowed (or any other message you want to provide), during interactive logon.	Low	Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows NT\ Current Version\Winlogon\ Add Value: LegalNoticeCaption Type: REG_SZ String: "Whatever you want for the title of the message box" Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows NT\ Current Version\Winlogon\ Add Value: LegalNoticeText Type: REG_SZ String: "Whatever you want for the text of the message box"

Registry Permissions

Note: *Unless it is specifically stated to remove a group, do not remove group memberships. Under the Changes column, "Set" refers to a modification of existing privileges while "Add" and "Delete" are adding new entries and deleting existing entries.*

Item	Purpose	Priority	Changes
Registry Permissions			
Restrict remote access to registry	Controls access to the registry over the network. Only administrators should have any remote access to the registry.	High	Key: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\SecurePipeServers\ Value: winreg Add Administrators: Full Control Delete: All other Users and Groups
Restrict unauthorized users from creating shares.	Allows administrator to control who can access a host from its network interface and what information can be accessed.	High	Key: HKEY_LOCAL_MACHINE\SYSTEM\ Sub-key: CurrentControlSet\ Services\LanmanServer\Shares\ Set Everyone: Read (at most) Set all untrusted users: Read (at most)
Restrict access to critical Run keys	Prevents unauthorized users from planting trojan executables during automated operations such as installation or uninstallation procedures.	Med	Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\ Sub-Keys: Run\, RunOnce\, RunOnceEx, Uninstall\, (if present), AEDebug\, Winlogon\ - and all their subkeys Set Everyone: Read (at most) Set all untrusted users: Read (at most)
Restrict user access to Software\ sub-key	This change is recommended. It locks the system in terms of who can install software. Note: It is not recommended that the entire subtree be locked using this setting because it can render certain software unusable	Med	Key: HKEY_LOCAL_MACHINE\ Sub-key: Software\ NOTE: Do not set on all subkeys of Software, or you may render certain software unusable! Set Everyone: Read (at most) Set all untrusted users: Read (at most)
Restrict user access to RPC sub-key	This change is recommended. It locks the RPC services.	Med	Key: HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ Sub-keys: RPC\ (and all its sub-keys) Set Everyone: Read (at most) Set all untrusted users: Read (at most)

Item	Purpose	Priority	Changes
Restrict user access to Read-only on critical registry keys	The following changes are recommended for a high security environment. Due to the nature of these changes, rigorous testing should be done with all user-supported applications to insure that proper access is allowed.	Low	Key: HKEY_LOCAL_MACHINE\ Sub-Keys: \Software\Microsoft\Windows NT\ CurrentVersion CurrentVersion\ProfileList CurrentVersion\AeDebug CurrentVersion\Compatibility CurrentVersion\Drivers CurrentVersion\Embedding CurrentVersion\Fonts CurrentVersion\FontSubstitutes CurrentVersion\Font Drivers CurrentVersion\Font Mapper CurrentVersion\Font Cache CurrentVersion\GRE_Initialize CurrentVersion\MCI CurrentVersion\MCI Extensions CurrentVersion\PerfLib CurrentVersion\Port (and all subkeys) CurrentVersion\Type1 Installer CurrentVersion\WOW (and all subkeys) CurrentVersion\Windows3.1MigrationStatus (and all subkeys) Key: HKEY_LOCAL_MACHINE\ Sub-Keys: \System\CurrentControlSet\Services\ LanmanServer\Shares UPS Key: HKEY_LOCAL_MACHINE\ Sub-Keys: \Software\Microsoft\Windows\ Key: \HKEY_CLASSES_ROOT\ Sub-Keys: All subkeys Key: HKEY_USERS\ Sub-Keys: Default\ Set Everyone: Read (at most) Set all untrusted users: Read (at most)

File System Permissions

File Permissions in the System Folder should be restricted to prevent unauthorized access and/or modifications. While the default installation provides some level of security control on these files, environments requiring a high level of security should make the following modifications. As with any of the *high* security changes that are implemented, be sure to thoroughly test your standard builds before implementing on production servers.

Note: *The following permissions are not just reflecting changes to be made but are the only permissions that should exist on these directories after changes are made.*

Directory	Permissions	Priority
\WINNT and *all subdirectories* under it.	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control	Med

Within the \WINNT tree, apply the following exceptions to the general security:

Directory	Permissions	Priority
\WINNT\REPAIR	Administrators: Full Control	High
\WINNT\SYSTEM32\CONFIG	Administrators: Full Control CREATOR OWNER: Full Control Everyone: List SYSTEM: Full Control	Med
\WINNT\SYSTEM32\SPOOL	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control	Med

\WINNT\COOKIES \WINNT\FORMS \WINNT\HISTORY \WINNT\OCCACHE \WINNT\PROFILES \WINNT\SENDTO \WINNT\Temporary Internet Files	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Special Directory Access – Read, Write and Execute, Special File Access – None System : Full Control	Low

Several critical operating-system files exist in the root directory of the system partition on Intel 80486 and Pentium-based systems. In high-security installations you may want to assign the following permissions to these files:

File	Permissions	Priority
\Boot.ini, \Ntdetect.com, \Ntldr	Administrators: Full Control SYSTEM: Full Control	High
\Autoexec.bat, \Config.sys	Everybody: Read Administrators: Full Control SYSTEM: Full Control	High
\TEMP directory	Administrators: Full Control SYSTEM: Full Control CREATOR OWNER: Full Control Everyone: Special Directory Access – Read, Write and Execute, Special File Access – None	Med

User Rights

In environments requiring a high level of security, make the following changes to default user rights:

User Right	Groups assigned this right by default on workstation & stand-alone server	Recommended change for workstation & stand-alone server	Groups assigned this right by default on domain controller	Recommended change for domain controller
Log on locally	Administrators, Everyone, Guests, Power Users and Users	Remove Everyone and Guests	Account Operators, Administrators, Backup Operators, Server Operators and Print Operators	No Change
Shut down the system (SeShutdownPrivilege)	Administrators, Everyone, Guests, Power Users and Users	Remove Everyone, Guests and Users.	Account Operators, Administrators, Backup Operators, Server Operators and Print Operators	No Change
Access this computer from the network	Administrators, Everyone and Power Users	Administrators, Power Users and Users	Administrators and Everyone	Administrators, Backup Operators, Server Operators, Print Operators, Users and Guests if it is enabled

Appendix B – Resources and Tools

Resources

Microsoft's Security Sites:
http://www.microsoft.com/security/
http://www.microsoft.com/technet/security/

Microsoft's C2 Security:
http://www.microsoft.com/technet/security/c2eval.asp
http://www.microsoft.com/technet/security/C2config.asp
http://www.microsoft.com/NTServer/security/exec/feature/c2_security.asp

Microsoft Service Pack 6a Bug Fix List:
http://support.microsoft.com/support/kb/articles/q241/2/11.asp

Microsoft's Hotfix Site:
http://support.microsoft.com/servicedesks/hotfixes/nts_hf_public_new.asp
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postsp6a/

Miscellaneous Security Sites:
http://www.sans.org/
http://www.securityfocus.com/
http://www.cert.org/
http://www.technotronic.com/
http://packetstorm.securify.com/
http://securityportal.com/

Tools

NT Resource Kit (only updates here):
http://www.microsoft.com/ntserver/nts/downloads/recommended/ntkit/default.asp

Microsoft Security Configuration Manager (SCM):
http://www.microsoft.com/TechNet/winnt/Winntas/technote/scmnt4.asp

Event Logging:
http://www.eventreporter.com/

Vulnerability Assessment Tools:
ISS Internet Scanner
http://www.iss.net/securing_e-business/security_products/security_assessment/

Network Associates Cybercop Scanner
http://www.pgp.com/products/cybercop-scanner/

Bindview
http://www.bindview.com/

Binary Integrity Checkers

TripWire
http://www.tripwire.com/
Intrusion Detection

ISS Realsecure
http://www.iss.net/securing_e-business/security_products/intrusion_detection/

Cybersafe Centrax
http://www.cybersafe.com/solutions/centraxoverview.html