Securing (Hardening) Windows Servers

A Whitepaper

By

Business Advisory Services
Information Security

JP Vossen, CISSP

7 Ridgedale Avenue
Cedar Knolls, NJ 07927

800-AlphaNet
security@alphanetsolutions.com
http://www.alphanetsolutions.com/

Contents

Introduction

Information Security is often seen as a cost center that produces very little in the way of return on investment (ROI). This is unfortunate, because when properly aligned with the business, Information Security can enable many things that before were too slow, too risky or simply not possible.

What business today operates with no insurance? Virtually none. Yet Information Security helps mitigate risk, exactly like insurance, and it also enables new ways of interacting with clients, partners and employees.

There are three very broad ways to classify companies right now:

- Those who do not use the Internet, because of fear of the security risks;
- Those who do use the Internet, and ignore the security risks;
- Those who understand the security risks, take steps to reduce and eliminate those risks, and then take full advantage of the Internet.

Which group do you belong to? Which group do you **want** to belong to? What does this have to do with hardening servers?

Information Security is a never-ending circular process, there are no silver bullets, and it is fundamentally not a technical problem that may be "solved" with point products[1]. This is not to say that there are not technical problems with technical solutions. It's just that the technical issues are only part of the problem. One of the most interesting technical problems that does exist and that may be addressed (not solved, but addressed) is host or server security. Most of the electronic data that we are interested in protecting resides, in some way, on a server somewhere. How well is that server protected?

Effective security is always layered. Some of the most common layers include:

- User authentication (passwords);
- Access controls (permissions);
- Firewalls;
- Intrusion Detection Systems (IDS);
- And you guessed it—server hardening.

What is Hardening?

- Has nothing to do with "Viagra!"
- Hardening is the process of tightening the security of an operating system from the default "out of the box" configuration to an appropriately secure level.
- Sometimes known as securing or locking down.

Why should I do it?

- Most modern Operating Systems are configured for ease-of-use—NOT Security—out of the box.
- One part of a "Security in Depth" or layered approach

[1] http://www.jpsdomain.org/security/principles.html

- "Security through Obscurity" is NO security at all!
  - NBT Name Scans (port 139/TCP) on my iDSL link at my house:
    - Sep 2001: 34 (1.1/Day)
    - Oct 2001: 160 (5.2/Day)
    - Nov 2001: 96 (3.2/Day)
    - Dec 2001: 82 (2.6/Day)
    - Jan 2002 (to 1/21/02): 45 (2.0/Day)
- Hardening is a demonstration of "reasonable and prudent precautions"
- The latest CSI/FBI Computer Crime and Security Survey 2001[2] has the following notes (emphasis added).

> "Conventional wisdom says "80% of computer security problems are due to insiders, 20% are due to outsiders."
> […]
> "But for the fourth year in a row, more respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%). Indeed, the numbers of those citing their Internet connection as a frequent point of attack has been rising, while the number of those reporting both dial-up remote access and their own internal systems as a frequent point of attack has been declining."
>
> "As Georgetown's Dr. [Dorothy] Denning comments, other results from this year's survey seem to underscore this trend."
>
> > *One interesting trend is the shift of the perceived threats from insiders to outsider. For the first time, more respondents said the independent hackers were more likely to be the source of an attack than disgruntled or dishonest insiders (81% vs 76%). Perhaps the notion that insiders account for 80% of incidents no longer bears any truth whatsoever."*
>
> "The number of respondents who reported incidents of "unauthorized access by insiders" within the last twelve months also dropped from 71% in 2000 to 49% in 2001."
>
> "Clearly, the threat from the outside is increasingly dramatically [*sic*] and has been doing so for several years."
>
> **"But is the threat from the inside actually decreasing?"**
>
> **"It would be premature and dangerous to assume so."**

Why Should I Harden Internal Servers?

For all of the reasons above. Remember that an action does not have to be malicious to have a negative effect. In the old days, it was easy to type "`del *.*`" in the wrong place and destroy your machine. It's not much harder to make the same mistake in an Explorer window. If the server is not appropriately secured, you can take a lot of other people's data down with you.

As much as we want to trust our employee's and believe it can't happen here, statistically it can. Especially in this economic climate, where cutbacks of all kinds are all too common, it **can** happen here.

[2] http://www.gocsi.com/forms/fbi/pdf.html

A Generic Hardening Process

Pre-implementation: Segregation of Data.

This is most important for web servers, but it does apply to other servers as well. Another term would be compartmentalization, and it has to do with the sensitivity (e.g. classification) of the information, and who has access to it.

The classic case is that of a database back-end to an Internet web server front end. You never want to have the database on the web server. Web servers are relatively easy to compromise, so critical data must never be stored on them. Ideally, the web server is behind a firewall, and the database is behind another firewall (or the same firewall, but on a different network/interface). The firewall rules allow the database to provide the web server with information, but if the web server is compromised, the attacker can't just copy the entire database (perhaps containing credit cards) right off the web server.

The same concepts hold true even for internal servers. You probably want to keep the HR and Accounting information on a different server than the general file and print servers. It's just too easy to make a simple mistake with permissions that allows the wrong people to access such sensitive information.

Implementation/Installation: Install Only Things that are Absolutely Necessary

Any service that is not installed cannot be compromised. Don't install SNMP (Simple Network Management Protocol), NetBEUI, Network Monitor, etc. if they are not needed. Likewise, many management programs, such as Compaq's Insight Manager, install a mini-web server by default. **Don't install those, especially on sensitive servers!**

Hardening:

Install all Service Packs/Hotfixes, etc.

This one is obvious, but sometime overlooked because it is so tedious. The WindowsUpdate[3] site and the Hfnetchk[4] tool make this much easier.

Disable all unnecessary services/devices/accounts

Any service that is not running cannot be compromised. But be aware that simply changing a service to startup "manually" may not be enough—those services may be started by the system if it decides they are needed… **Disable** any service that is not essential.

See the "Table of Services" on page 16 for information about services. Devices and accounts are too specific to each machine and environment to really say too much about them. When in doubt, turn it off and test it!

Enable Appropriate Password Settings

Windows NT stores passwords in the SAM (Security Accounts Manager) file. Windows 2000 Domain Controllers use Active Directory, but non-DCs still use the SAM. By default, 2000 uses SysKey encryption on the SAM, which somewhat complicates the method of obtaining password hashes.

[3] http://windowsupdate.microsoft.com/
[4] http://support.microsoft.com/support/kb/articles/q303/2/15.asp

Pwdump v2 allows even SysKey encrypted SAMs to be dumped, but only on the local machine. Pwdump v3 allows remote dumping, though both versions require administrative access, as well as special User Rights. Syskey was introduced with NT4 SP3, but is not enabled by default on NT 4.0. There was also at least one vulnerability that has been corrected in a post-SP6 hotfix (Syskey Tool Reuses Keystream [Q248183]).

Both NT and 2000 store two versions of the password hash, LanMan and NTLM (NT LanMan). The LanMan hash is needed for backward compatibility for Windows 9x clients, but is very weak. Among its many problems, it stores all the passwords in upper case, so password case does not matter.

Given this, the most secure passwords are either exactly 7 or exactly 14 characters. An 8 or 9 character password is actually **less secure** than an exactly 7 character password, given the way they are stored, and the way L0phtCrack attacks them!

For administrative and service accounts, I recommend exactly 14 character passwords. For regular user accounts, you may as well set it at 7 and forget it, since there is a zero percent chance you will get 100% compliance, no matter what you do[5].

Be especially careful of service accounts! Everyone I know who does penetration studies, including me, has been able to hack into a system by guessing at service account passwords at least 70% of the time!

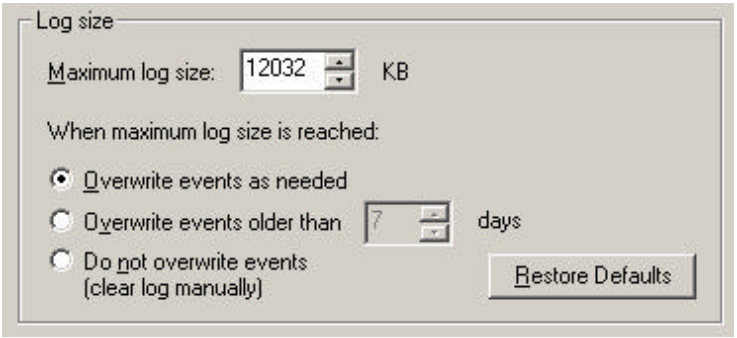
You can use the "net accounts" command to modify password settings:

```
NET ACCOUNTS /MINPWLEN:7 /MAXPWAGE:2 /MINPWAGE:1 /UNIQUEPW:10 /FORCELOGOFF:1
      /LOCKOUTTHRESHOLD:3 /LOCKOUTDURATION:99999 /LOCKOUTWINDOW:600
```

Enable Appropriate Logging/Auditing

By default logging is not enabled. Turning it on after an incident is as bad as locking the door after the horse is gone. Turn it on now, even if you ignore it, which you shouldn't. You will also need to increase the log size from the default 512 KB. I recommend about 12 Meg, and "Overwrite as needed."

Many security professionals will disagree with that last setting. I don't like it myself, but something is better than nothing. If you actually monitor your logs, by all means use a better setting. If you do not log, or if you ignore the logs, then enable logging and use this setting. It's zero maintenance, and it's a reasonable policy for when (not if) something happens. Occasionally archiving logs is also a good practice (see "Tools" on page 14 for free and Resource Kit tools to facilitate this task).



[5] See Peter Tippet's *Stronger Passwords Aren't* http://www.infosecuritymag.com/articles/june01/columns_executive_view.shtml.

Policy	Local Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Failure
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

You can use the SCE/SCM (Security Configuration Editor/Security Configuration Manager) on NT 4.0, the "Local Security Policy, Audit Policy" on Windows 2000 or the Resource Kit "auditpol" utility (all) to modify logging settings:

```
auditpol /enable /System:all /Logon:all /Object:failure /Privilege:failure
      /Process:none /Policy:all /Sam:all
```

The following will fail under NT4, giving the oh so useful error message "... This function is only valid in Windows NT Mode."

```
auditpol /Directory:failure /Account:all
```

You can also use my Windows port of the famous UNIX Logcheck log monitoring tool[6], which will e-mail "suspicious" or interesting log entries to you.

Use the Concept of "Least Privilege"

This is pretty easy. Don't add more accounts to the administrator groups than absolutely necessary. Especially, try to avoid adding service accounts to the administrator groups if at all possible. Some service accounts (e.g. SMS or SQL) may require administrative privileges, while others (e.g. Exchange) do not. I know what a pain it is to research and figure out just what rights and access is required (since practically no vendor tells you this information). But it is worth it. Remember, I can almost always get into your system right away using service accounts—when they are in the administrator groups, your network is toast in 5 minutes or less!

Also, under NT 4.0 and 2000, the "Everyone" Group really means "everyone who can get a packet to the machine!" Avoid it, even though it is used be default. Try to substitute the "Authenticated Users" or "Domain Users" groups. But be aware that this can potentially break some anonymous browsing (e.g. Network Neighborhood). See "The Importance of Testing!" on page 8. (Windows XP has a new setting that can lock the "Everyone" group down a bit better.)

Enable "Extra" Security Settings

When you read the Microsoft best practices and checklists in the reference section below, you will find all kinds of neat settings you can tweak. Two easy examples are the "Do not display last user name in logon screen" and warning banners. These settings are exposed in "Local Security Policy, Local Policies, Security Options" in 2000, but you have to tweak the registry (or use SCE/SCM) in NT 4.0.

[6] http://www.jpsdomain.org/winlogcheck/

Tighten NTFS/Registry Permissions

OK, this one is the killer. One of the easiest ways I know to render a Windows server useless is to start playing around with the NTFS and Registry permissions. That said, by default they are pretty open. See "The Importance of Testing!" on page 8 and "Hardening Windows Links" on page 14.

Implement Time Synchronization

ISO/IEC 17799:2000(E)[7] (AKA BS7799), clause "9.7.3 Clock synchronization:"

> The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence.
>
> Where a computer or communications device has the capability to operate a real-time clock, it should be set to an agreed standard, e.g. Universal Coordinated Time (UCT) or local standard time. As some clocks are known to drift with time, there should be a procedure that checks for and corrects any significant variation.

See my page on NTP Time Synchronization[8], which covers use of the "net time" command, and lists free (S)NTP clients and servers for Windows, including the excellent NTRK timeserv tool[9].

The Importance of Testing!

- It is extremely easy to corrupt a Windows system beyond recovery when hardening it.
  - NTFS Permissions
  - Registry settings/permissions
- Never attempt to establish or test hardening procedures on a production box! Ever!
- Ghost is your friend!
- Did I mention "Never attempt to establish or test hardening procedures on a production box?"
- Ever!

Differences between NT 4.0 and 2000 (e.g. SCE/SCM)

- In NT 4.0 SCE/SCM is not available by default. It was first made available on the SP4 CD-ROM.
- It was back-ported from 2000.
- It changes the NT 4.0 NTFS permissions DLL from the old NT 4.0 style to the new Windows 2000 style—e.g. inherited permissions. This is not always desirable.
- The un-patched version has significant bugs and issues. See "Some Issues with MMC SCM/SCE Corrected in SP6a" on page 16.

Hardening Internal Servers

- Never install IIS unless the server is to be a dedicated Web Server, and then segregate data!
- Hardening:
  - Install all Service Packs/Hotfixes, etc.
  - Disable all unnecessary services/devices/accounts (see the "Table of Services" on page 16)
  - Enable appropriate logging/auditing

[7] http://www.bspsl.com/17799/
[8] http://www.jpsdomain.org/time/
[9] http://www.niceties.com/time.html

  - Use the concept of "Least Privilege"
    - Admin Accounts
    - User Rights (Beware the "Everyone" Group!)
  - Consider enabling "extra" security settings
  - Consider tightening NTFS/Registry permissions
- See "Hardening Windows Links" on page 14.

Hardening IIS Servers

- Never install IIS unless the server is to be a dedicated Web Server, and then segregate data!
- Perform all hardening as above for an internal server, except more stringently.
- Consider moving critical tools out of default locations (see "MoveTools.cmd" on page 11).
- Harden IIS. See "Hardening IIS Links" on page 15 and the "Table of Services" on page 16.

Hardening Windows to be a Firewall Platform

- A firewall server must be a dedicated box running only the firewall software (e.g. no DNS, FTP, etc.)!
- Never, ever, EVER run IIS on a firewall server!
- Perform all hardening as above for an internal server, except more stringently.
- Disable NBT (AKA MS Networking, see "How to Disable NBT" on page 9).
- Disable virtually all services and devices (see the "Table of Services" on page 16).
- Lock down NTFS permissions (this is easy, since you don't have to worry about users, only Administrators and System!).
- Consider moving critical tools out of default locations (see "MoveTools.cmd" on page 11).
- See "Firewall Hardening Links" on page 15.

Resources and References

How to Disable NBT

This section was originally written for NT 4.0, but the process is essentially the same for Windows 2000.

Recommendations

- ***Make sure you have a valid backup of the entire system before you attempt any of these procedures!***
- Read the warning below very carefully, and fully understand what it means.
- Test this procedure on a non-production box to ensure that it works as expected.

Warning

This configuration is not recommended for internal servers, such as Intranet Web Servers, as certain functionality is severely limited for security reasons. This may be overkill on the internal network.

The following procedure will disable all Microsoft Networking components of NT. This means the Server will be **unable** to:

- Run the MS DNS service (which depends on WINS, which depends on the server service, workstation service, the RPC service and NetBIOS).
- Use the GUI Interface "WinAT" (NT Resource Kit utility) which depends on the Workstation Service. "AT" still works, though unless it is needed for certain log (switching) functions it

should be disabled. The Windows 2000 "Windows Time Service" has no dependencies and will work fine.

- Use the NTRK TimeServ NTP time server or client (which depends on the workstation service).
- Join a Domain or Workgroup.
- Run Server Manager (all other NT Administration tools will function, mostly).
  - UserManager will give an error message when you run that the workstation driver is not installed. Ignore it, and specify the machine name as the new domain to administer, e.g. \\Mynewserver.) See "How to Re-Enable the Workstation Service" on page 11 if necessary.
  - If you get a UserManager message that the "workstation driver is not loaded" when creating a new User, you have made an error, but UserManager depends on the workstation service for displaying error codes. The most likely error is that you have either not created a password, or your password does not meet complexity requirements. Use upper and lower case with numbers and punctuation.
- Browse any network.
- Map (net use) any remote drives.
- Use NetBEUI/NetBIOS MS/NT functions.
- Use RPC functions.

Remove Unneeded Network Services

1. Clear the Event Log (optional).
2. Reboot the server. If any error messages appear (such as "A service failed to start…") correct them. Do not continue until the server boots up cleanly.
3. Go to Start, Settings, Control Panel, Network.
4. Choose the "Protocols" tab.
5. If there are any protocols other than TCP/IP, remove them, and re-boot. Begin with this section again when the server comes up.
6. Go to Start, Settings, Control Panel, Network.
7. Choose the "Bindings" tab and "Show Bindings for: All Services".
8. Disable everything (usually NetBIOS Interface, Workstation, Server).
9. "Show Bindings for: All Adapters".
10. Disable WINS Client (TCP/IP).

Remove Other Devices and Services

1. Go to Start, Settings, Control Panel, Devices.
2. Stop the "NetBIOS Interface".
3. Choose the [STARTUP] button, then select Disabled for that device.
4. Stop the "WINS Client (TCP/IP)".
5. Choose the [STARTUP] button, then select Disabled for that device.
6. Reboot the server. If it comes up cleanly, with no error messages (such as "A service failed to start…") you were successful. You now have an NT server that can communication only via TCP/IP. If there were error messages, check the Event Log for details, than go back and make sure you did not miss removing or disabling a service.

Verification

1. From a command prompt, type "netstat –an" and make sure no ports below 1024 are "LISTENING". Port 135 UDP and TCP will be listening – this is RPC and it causes problems if you disable or remove it. If you have installed a firewall or other service, it will probably be listening on some ports as well. If any other ports are listening, you missed a service. Especially look for 21 (FTP); 25 (SMTP); 80 (Web server); 137, 138, 139 (MS Networking); 445 (MS Directory Services).
2. Check Control Panel, Services and make sure nothing is started that does not need to be.
3. Check Control Panel, Devices, and make sure nothing is started that does not need to be.

How to Re-Enable the Workstation Service

Do **NOT** do this on a production server and leave it this way – that is a breach of security! Again, this section was originally written for NT 4.0, but the process is essentially the same for Windows 2000.

1. Go to Start, Settings, Control Panel, Network.
2. Choose the "Bindings" tab and "Show Bindings for: All Services".
3. Enable the Workstation bindings only.
4. Hit [OK] and close out of the Network box.
5. **You do NOT have to reboot when prompted!**
6. Go to Start, Settings, Control Panel, Services.
7. Change the Workstation startup from disabled to manual.
8. Start the Workstation service and do whatever you need to do.
9. When finished, disable everything you just re-enabled.

Note: even though you are told several times you have to reboot, you do not. However, on NT if you do this too often, sooner or later you'll have problems. Reboot if possible, at least once you are finished.

MoveTools.cmd

Note, you must manually set NTFS permissions on the directory to which you move the tools (e.g. c:\AdminTools). You can download this Whitepaper and the batch file below from http://www.jpsdomain.org/jp/.

```
@echo off
REM MoveTools.cmd -- implement Step 2 "Copy and ACL Critical Files" recommended
REM by the following URL:
rem    http://www.microsoft.com/technet/security/tools/iischk.asp
rem See Also the other checklists at (much redundant info between them,
rem    but each is also a little different!):
rem    http://www.microsoft.com/technet/security/tools.asp

rem Copyright 2000 JP Vossen (http://www.jpsdomain.org/)
rem Licensed under the GNU GENERAL PUBLIC LICENSE:
rem    See http://www.gnu.org/copyleft/gpl.html for full text and details.

rem v1.0 22-Dec-2000 JP Vossen jp@jpsdomain.org
rem v1.1 08-Feb-2001 JPV Added more files, bug fixes and work-arounds
rem v1.2 21-Feb-2001 JPV Added more files from NSA Guide, update URL

REM Add Other NT4 Admin Tools?!?

rem ======================================================

if "%1" == "?"      goto Usage
if "%1" == "/?"     goto Usage
if "%1" == "-h"     goto Usage
```

```
if "%1" == "--help" goto Usage

rem ======================================================
REM Set the directory to create and copy the files to.
REM Note you must use this same directory in "SetPath.cmd".

if     "%1" == "" Set AdminTools=c:\AdminTools
if NOT "%1" == "" Set AdminTools=%1

rem ======================================================

if not exist %AdminTools%\NUL md %AdminTools%

echo.
echo.
echo on
move %SYSTEMROOT%\regedit.exe           %AdminTools%
move %SYSTEMROOT%\System32\arp.exe      %AdminTools%
move %SYSTEMROOT%\System32\at.exe       %AdminTools%
move %SYSTEMROOT%\System32\atsvc.exe    %AdminTools%
move %SYSTEMROOT%\System32\cacls.exe    %AdminTools%
move %SYSTEMROOT%\System32\cmd.exe      %AdminTools%
move %SYSTEMROOT%\System32\cscript.exe  %AdminTools%
move %SYSTEMROOT%\System32\debug.exe    %AdminTools%
move %SYSTEMROOT%\System32\edit.com     %AdminTools%
move %SYSTEMROOT%\System32\edlin.exe    %AdminTools%
move %SYSTEMROOT%\System32\finger.exe   %AdminTools%
move %SYSTEMROOT%\System32\ftp.exe      %AdminTools%
move %SYSTEMROOT%\System32\ipconfig.exe %AdminTools%
move %SYSTEMROOT%\System32\nbtstat.exe  %AdminTools%
move %SYSTEMROOT%\System32\net.exe      %AdminTools%
move %SYSTEMROOT%\System32\netstat.exe  %AdminTools%
move %SYSTEMROOT%\System32\nslookup.exe %AdminTools%
move %SYSTEMROOT%\System32\ping.exe     %AdminTools%
move %SYSTEMROOT%\System32\posix.exe    %AdminTools%
move %SYSTEMROOT%\System32\qbasic.exe   %AdminTools%
move %SYSTEMROOT%\System32\rcp.exe      %AdminTools%
move %SYSTEMROOT%\System32\rdisk.exe    %AdminTools%
move %SYSTEMROOT%\System32\regedt32.exe %AdminTools%
move %SYSTEMROOT%\System32\rexec.exe    %AdminTools%
move %SYSTEMROOT%\System32\route.exe    %AdminTools%
move %SYSTEMROOT%\System32\rsh.exe      %AdminTools%
move %SYSTEMROOT%\System32\runonce.exe  %AdminTools%
move %SYSTEMROOT%\System32\secfixup.exe %AdminTools%
move %SYSTEMROOT%\System32\syskey.exe   %AdminTools%
move %SYSTEMROOT%\System32\telnet.exe   %AdminTools%
move %SYSTEMROOT%\System32\tracert.exe  %AdminTools%
move %SYSTEMROOT%\System32\wscript.exe  %AdminTools%
move %SYSTEMROOT%\System32\xcopy.exe    %AdminTools%

@REM Files from NSA "The 60 Minutes Network Security Guide")
move %SYSTEMROOT%\System32\net1.exe     %AdminTools%
move %SYSTEMROOT%\System32\netsh.exe    %AdminTools%
move %SYSTEMROOT%\System32\regsvr32.exe %AdminTools%
move %SYSTEMROOT%\System32\runas.exe    %AdminTools%
move %SYSTEMROOT%\System32\sysedit.exe  %AdminTools%
move %SYSTEMROOT%\System32\tftp.exe     %AdminTools%
move %SYSTEMROOT%\System32\xcopy.exe    %AdminTools%
move %SYSTEMROOT%\System32\xcopy.exe    %AdminTools%

@REM Files added by JPV
move %SYSTEMROOT%\poledit.exe           %AdminTools%
move %SYSTEMROOT%\System32\append.exe   %AdminTools%
```

```
move %SYSTEMROOT%\System32\attrib.exe   %AdminTools%
move %SYSTEMROOT%\System32\doskey.exe   %AdminTools%
move %SYSTEMROOT%\System32\find.exe     %AdminTools%
move %SYSTEMROOT%\System32\findstr.exe  %AdminTools%
move %SYSTEMROOT%\System32\mmc.exe      %AdminTools%
move %SYSTEMROOT%\System32\pathping.exe %AdminTools%
move %SYSTEMROOT%\System32\recover.exe  %AdminTools%
move %SYSTEMROOT%\System32\replace.exe  %AdminTools%
move %SYSTEMROOT%\System32\setver.exe   %AdminTools%
move %SYSTEMROOT%\System32\subst.exe    %AdminTools%
move %SYSTEMROOT%\System32\winmsd.exe   %AdminTools%

@echo off

rem ========================================================
rem Create the "SetPath.cmd" batch file

echo @echo off > %AdminTools%\SetPath.cmd
echo REM SetPath.cmd -- Set the path to admin tools for a DOS Prompt session.
       >> %AdminTools%\SetPath.cmd
echo rem v1.0 08-Feb-2001 JP Vossen jp@jpsdomain.org >>
       %AdminTools%\SetPath.cmd
echo. >> %AdminTools%\SetPath.cmd
echo REM Note the directory must be the same as that set in "MoveTools.cmd". >>
       %AdminTools%\SetPath.cmd
echo. >> %AdminTools%\SetPath.cmd
echo path=%AdminTools%;%path% >> %AdminTools%\SetPath.cmd


rem ========================================================
goto Exit
:Usage

echo.
echo.
echo Usage: %0 {Directory to move files to}
echo.
echo   E.G. %0 c:\AdminTools      (The default if not specified)
echo.

rem ========================================================
:Exit
REM Clean up
Set AdminTools=
```

Books

Norberg, Stefan, *Securing Windows NT/2000 Servers for the Internet*, O'Reilly, November 2000.

McClure, et al., *Hacking Exposed: Network Security Secrets & Solutions Third Edition*, Osborne, 2001.

Sheldon, Tom, *Windows NT Security Handbook 2nd Edition*, Osborn, June 1998

URLS

Resource	Comment
http://www.jpsdomain.org/jp/	This Whitepaper in PDF format, under "Publications & Whitepapers"
http://www.faqs.org/rfcs/rfc1244.html	Handbook of computer security and procedures
See http://www.infosecuritymag.com/	Windows Security Scripting" article in the February issue of Information Security Magazine.

Resource	Comment
http://www.portsdb.org/	Search for port numbers and names
http://www.snort.org/ports.html	Search for port numbers and names

Tools

Tool Resources	Comment
http://www.jpsdomain.org/winlogcheck/	WinLogCheck, my Windows port of the UNIX logcheck log monitoring tool
http://www.somarsoft.com/somarsoft_main.htm#DumpEvt	DumpEvt, a free tool to dump Event Logs into a useful (ASCII) format.
ElogDmp.exe Dumpel.exe	Windows Resource Kits tools to dump the event log
EventLog.pl EventQuery.pl	Perl scripts to dump or query the Event Logs, included in the Win2K Server Resource Kit.

Hardening Windows Links

Hardening Windows Resources	Comment
http://www.microsoft.com/security/	**Microsoft Security Advisor**
http://www.microsoft.com/technet/security/tools.asp	**Tools and Checklists**
http://support.microsoft.com/support/kb/articles/Q303/2/15.ASP	HFNetChk (CLI net scanner against MS XML DB) [Very cool!]
http://www.microsoft.com/technet/security/tools/mpsa.asp	Microsoft Personal Security Advisor (MPSA)
http://windowsupdate.microsoft.com/	Download the latest Windows patches, customized for your specific computer
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp	A Single location for all MS Security Patches
http://www.trustedsystems.com/tss_nsa_guide.htm	**NSA Guide to Securing Windows NT (Oct. 1999, 123 pages)**
http://nsa1.www.conxion.com/index.html	**NSA Security Recommendation Guides: Windows 2000, NT 4.0, Cisco Routers, E-Mail, etc.**
http://www.sans.org/newlook/publications/ntstep.htm	**SANS – Windows NT Security: Step-by-Step (July 1999, 36 pages)**
http://www.sans.org/newlook/publications/index.htm	**SANS – Windows 2000 Security: Step-by-Step and Windows 2000 Security: Vulnerabilities and Solutions**
https://infosec.navy.mil/COMPUSEC/ntsecure.html	**US Navy – Secure Windows NT 4.0 Installation and Configuration Guide (May 1999, Dec. 1998)**
http://www.mcp.com/files/1-57870/1-57870-045-0/0450.zip	Automating NT installations (Sample Scripts and Registry files)
On NT4SP4 CD-ROM, or NT4SP6a (non-128 bit) CD-ROM or ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/SCM/	Where to obtain SCM/SCE
http://www.microsoft.com/ntserver/techresources/security/Secure_NTInstall.asp	Microsoft Guide to Securing Win NT
http://www.microsoft.com/ntserver/techresources/security/SecurConfigToolSet.asp	Microsoft Security Configuration Tool Set (SCTS) Paper (NT5)
http://www.microsoft.com/ntserver/techresources/security/securconfig.asp	Microsoft Security Configuration Manager (SCM) White Paper (NT4 SP4)
http://www.microsoft.com/technet/security/tools/c2config.asp	Microsoft Windows NT 4.0 C2 Configuration Checklist
http://www.microsoft.com/technet/security/tools/mbrsrvcl.asp	Windows NT 4.0 Member Server Configuration Checklist

Hardening Windows Resources	Comment
http://www.microsoft.com/technet/security/tools/wrkstchk.asp	Windows NT 4.0 Workstation Configuration Checklist
http://www.microsoft.com/technet/security/tools/nt4wscl.asp	Windows NT 4.0 Workstation Baseline Security Checklist
http://www.microsoft.com/technet/security/tools/nt4svrcl.asp	Windows NT 4.0 Server Baseline Security Checklist
http://www.microsoft.com/technet/security/tools/w2kprocl.asp	Windows 2000 Professional Baseline Security Checklist
http://www.microsoft.com/technet/security/tools/w2ksvrcl.asp	Windows 2000 Server Baseline Security Checklist
http://support.microsoft.com/support/kb/articles/Q148/4/37.asp	Default NTFS Permissions in Windows NT
http://www.microsoft.com/NTServer/nts/downloads/recommended/ntkit/default.asp	**A free subset of the NT4 Resource Kit tools**
http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp	**A free subset of the Win2K Resource Kit tools**

Hardening IIS Links

Hardening IIS Resources	Comment
http://www.microsoft.com/ technet/security/tools/iis5cl.asp	IIS 5.0 Baseline Security Checklist
http://www.microsoft.com/technet/security/tools/iis5chk.asp	Secure Internet Information Services 5 Checklist
http://www.microsoft.com/technet/security/tools/iis4cl.asp	Internet Information Server 4 Baseline Security Checklist
http://www.microsoft.com/technet/security/tools/iischk.asp	Microsoft Internet Information Server 4.0 Security Checklist
http://www.microsoft.com/TechNet/prodtechnol/iis/deploy/confeat/seciis50.asp	Securing IIS 5.0 Using Batch-Oriented Command Files
http://www.microsoft.com/windows2000/zipdocs/security.exe	Securing IIS 5.0 Using Batch-Oriented Command Files (Download the tools ZIP)
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/locktool.asp	IIS Lockdown Tool (Info)
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32362	IIS Lockdown Tool (Download)
http://www.infosecuritymag.com/articles/september01/features_IIS_security.shtml	Ten Steps to Better IIS Security
http://grc.com/pw/patchwork.htm	Detect certain common vulnerabilities in IIS
http://www.microsoft.com/TechNet/iis/iis5tune.asp	The Art and Science of Web Server Tuning with Internet Information Services 5.0
(Look for February 2002 issue on http://www.mcpmag.com/)	Souping Up Your IIS Server

Firewall Hardening Links

Firewall Hardening Resources	Comment
http://www.enteract.com/~lspitz/nt.html	Lance Spitzner's "Armoring NT"
http://www.enteract.com/~lspitz/	Lance's Security Papers
http://www.phoneboy.com/fw1/faq/0073.html http://www.elkrun.chantilly.va.us/ntsecurity/securent.html	PhoneBoy's Securing Windows NT FAQ
http://www.phoneboy.com/fw1/faq/0073-securent-steps.wri	Rush Wilson's "Secure NT – Steps.wri" (Note **WordPad Document**)

SCE/SCM Issues and Links

Search TechNet with the following query (DO use the double quotes):
"Security Configuration Editor" or "Security Configuration Manager"

Or, use one of the following URLs, using the appropriate article number at the end:
http://support.microsoft.com/support/kb/articles/Q195/5/09.asp
http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q195509

White Paper	MS Security Configuration Manager for Windows NT 4
Q195509	Installing (and **uninstalling**!) SCM from SP4 Changes Windows NT 4.0 ACL Editor
Q195227	SP4 Security Configuration Manager Available for Download
Q214752	Adding Custom Registry Settings to Security Configuration Editor
Q221074	Windows NT 4.0 SP4 ACL Editor Cannot Edit After Deleting a User
Q253382	Error Message: Unable to Display Security Information
Q225459	SP4 Security Configuration Manager Is Not Compatible with SBS

Some Issues with MMC SCM/SCE Corrected in SP6a

(MMC is Microsoft Management Console)

Q218934	Multiple Bugs in Security Configuration Manager MMC Snap-In
Q241489	User Right Incorrectly Configured in SCE High-Security Template
Q241719	Incorrect Analysis Information for Security Options in SCE
Q241653	Auditing Changes in SCM Not Reflected in User Manager Policies
Q240071	"Unable to Display Security Information" on Computer with SCM
Q232710	Privileges not Assigned if Two Users Start with Same Substring
Q222160	Security Configuration Editor Has Several UI-Related Problems

SysKey Issues and Links

Note: **There is no way to un-install SysKey.** See http://support.microsoft.com/support/kb/articles/Q143/4/75.asp for details pertaining to what registry and files changes are made, and the use of rdisk to provide some back-out and recovery options.

Q143475	Windows NT System Key Permits Strong Encryption of the SAM
Q248183	Syskey Tool Reuses Keystream

BindView Security Advisory: Vulnerability in Windows NT's SYSKEY
http://securityportal.com/list-archive/ntbugtraq/1999/Dec/0035.html

Table of Services

- The following lists are not complete lists of all possible services, nor do they list only services that are installed by default. Rather, they are representative samples of possible services you may see.
- Services **listed in bold** are particularly dangerous and/or interesting.
- **DO NOT ATTEMPT TO IMPLEMENT THESE RECOMMENDATIONS ON A PRODUCTION SERVER WITHOUT TESTING THEM ON <u>YOUR</u> CONFIGURATION(S) FIRST!**

NT 4.0

NT 4.0	Default		Sample Recommendation		
Display Name	**State**	**Start Mode**	**Internal**	**IIS**	**Firewall**
Alerter	Running	Automatic			Disable
ClipBook Server	Stopped	Manual	Disable if not used	Disable	Disable
Computer Browser	Running	Automatic			Disable
DHCP Client (TDI)	Stopped	Disabled	Disable if not used	Disable or remove	Disable or remove
Directory Replicator	Stopped	Manual	Disable if not used	Disable	Disable
EventLog (Event log)	Running	Automatic	Enable and configure	Enable and configure	Enable and configure
FTP Publishing Service	Running	Automatic	Disable if not used	Disable if not used	Disable or remove
Gopher Publishing Service	Running	Automatic	Disable if not used	Disable if not used	Disable or remove
License Logging Service	Stopped	Disabled		Disable if not used	Disable
Messenger	Running	Automatic			Disable
Net Logon (RemoteValidation)	Running	Automatic		Disable if not used	Disable
Network DDE (NetDDEGroup)	Stopped	Manual			Disable
Network DDE DSDM	Stopped	Manual			Disable
Network Monitor Agent	Stopped	Manual	Disable if not used	Disable if not used	Disable or remove
NT LM Security Support Provider	Running	Manual		Disable if not used	Disable
Plug and Play (PlugPlay)	Running	Automatic			
Protected Storage	Running	Automatic			
Remote Procedure Call (RPC) Locator	Running	Automatic	Don't touch	Don't touch	Don't touch
Remote Procedure Call (RPC) Service	Running	Automatic	Don't touch	Don't touch	Don't touch
Schedule	Stopped	Manual	Disable if not used	Disable if not used	Disable if not used
Server	Running	Automatic			Disable
Simple TCP/IP Services	Running	Automatic	Disable or remove	Disable or remove	Disable or remove
SNMP	Running	Automatic	Disable if not used	Disable if not used	Disable if not used
SNMP Trap Service	Stopped	Manual	Disable if not used	Disable if not used	Disable if not used
Spooler (SpoolerGroup)	Running	Automatic	Disable if not used	Disable	Disable
TCP/IP NetBIOS Helper	Running	Automatic		Disable	Disable

NT 4.0	Default		Sample Recommendation		
Display Name	**State**	**Start Mode**	**Internal**	**IIS**	**Firewall**
Telephony Service	Stopped	Manual	Disable if not used	Disable	Disable
UPS	Stopped	Manual	Disable if not used	Disable	Disable
Workstation (NetworkProvider)	Running	Automatic		Disable if not used	Disable
World Wide Web Publishing Service	Running	Automatic	Disable or remove	Disable if not used	Disable or remove

Windows 2000 Server

Win2000	Default		Sample Recommendation		
Display Name	**State**	**Start Mode**	**Internal**	**IIS**	**Firewall**
Alerter	Running	Auto			Disable
Application Management	Stopped	Manual			Disable
ClipBook	Stopped	Manual	Disable if not used	Disable or remove	Disable
COM+ Event System	Running	Manual			Disable
Computer Browser	Running	Auto			Disable
DHCP Client	Running	Auto	Disable if not used	Disable or remove	Disable or remove
DHCP Server	Running	Auto	Disable if not used	Disable or remove	Disable or remove
Distributed File System	Running	Auto			Disable
Distributed Link Tracking Client	Running	Auto	Disable if not used	Disable if not used	Disable
Distributed Link Tracking Server	Stopped	Manual	Disable if not used	Disable if not used	Disable
Distributed Transaction Coordinator	Running	Auto	Disable if not used	Disable if not used	Disable
DNS Client	Running	Auto			
DNS Server	Running	Auto	Disable if not used	Disable or remove	Disable or remove
Event Log	Running	Auto	Enable and configure	Enable and configure	Enable and configure
Fax Service	Stopped	Manual	Disable if not used	Disable if not used	Disable
File Replication	Stopped	Manual	Disable if not used	Disable if not used	Disable
FTP Publishing Service	Running	Auto	Disable if not used	Disable if not used	Disable or remove
IIS Admin Service	Running	Auto	Disable if not used	Disable if not used	Disable or remove
Indexing Service	Stopped	Manual	Disable if not used	Disable if not used	Disable or remove
Internet Connection Sharing	Stopped	Manual	Disable or remove	Disable or remove	Disable or remove

Win2000	Default		Sample Recommendation		
Display Name	**State**	**Start Mode**	**Internal**	**IIS**	**Firewall**
Intersite Messaging	Stopped	Disabled	Disable if not used	Disable if not used	Disable
IPSEC Policy Agent	Running	Auto	Disable if not used	Disable if not used	Disable if not used
Kerberos Key Distribution Center	Stopped	Disabled	Disable if not used	Disable if not used	Disable
License Logging Service	Running	Auto			Disable
Logical Disk Manager	Running	Auto			
Logical Disk Manager Administrative Service	Stopped	Manual			
Messenger	Running	Auto			Disable
Net Logon	Stopped	Manual		Disable if not used	Disable
NetMeeting Remote Desktop Sharing	Stopped	Manual	Disable or remove	Disable or remove	Disable or remove
Network Connections	Running	Manual		Disable if not used	Disable
Network DDE	Stopped	Manual			Disable
Network DDE DSDM	Stopped	Manual			Disable
NT LM Security Support Provider	Running	Manual		Disable if not used	Disable
Performance Logs and Alerts	Stopped	Manual	Disable if not used	Disable if not used	Disable if not used
Plug and Play	Running	Auto			
Print Spooler	Running	Auto	Disable if not used	Disable	Disable
Protected Storage	Running	Auto			
QoS RSVP	Running	Manual	Disable if not used	Disable if not used	Disable if not used
Remote Access Auto Connection Manager	Stopped	Manual	Disable if not used	Disable	Disable
Remote Access Connection Manager	Stopped	Manual	Disable if not used	Disable	Disable
Remote Procedure Call (RPC)	Running	Auto	Don't touch	Don't touch	Don't touch
Remote Procedure Call (RPC) Locator	Stopped	Manual	Don't touch	Don't touch	Don't touch
Remote Registry Service	Running	Auto	Disable if not used	Disable	Disable
Removable Storage	Running	Auto			
Routing and Remote Access	Stopped	Disabled	Disable if not used	Disable	Disable
RunAs Service	Running	Auto	Disable if not used	Disable if not used	Disable if not used
Security Accounts Manager	Running	Auto			
Server	Running	Auto			Disable

Win2000	Default		Sample Recommendation		
Display Name	**State**	**Start Mode**	**Internal**	**IIS**	**Firewall**
Simple Mail Transport Protocol (SMTP)	Running	Auto			Disable or remove
Simple TCP/IP Services	Running	Auto	Disable or remove	Disable or remove	Disable or remove
Smart Card	Stopped	Manual	Disable if not used	Disable if not used	Disable
Smart Card Helper	Stopped	Manual	Disable if not used	Disable if not used	Disable
SNMP Service	Running	Auto	Disable if not used	Disable if not used	Disable if not used
SNMP Trap Service	Stopped	Manual	Disable if not used	Disable if not used	Disable if not used
System Event Notification	Running	Auto			
Task Scheduler	Running	Auto	Disable if not used	Disable if not used	Disable if not used
TCP/IP NetBIOS Helper Service	Running	Auto		Disable	Disable
Telephony	Running	Manual	Disable if not used	Disable	Disable
Telnet	Stopped	Manual	Disable if not used	Disable	Disable
Terminal Services	Running	Auto	Disable or remove	Disable or remove	Disable or remove
Uninterruptible Power Supply	Stopped	Manual	Disable if not used	Disable if not used	Disable if not used
Utility Manager	Stopped	Manual			Disable
Windows Installer	Stopped	Manual		Disable if not used	Disable
Windows Internet Name Service (WINS)	Running	Auto	Disable if not used	Disable	Disable
Windows Mngmnt Instrumentation	Running	Auto		Disable if not used	Disable
Windows Mngmnt Instrumentation Drvr Ext.	Running	Manual		Disable if not used	Disable
Windows Time	Stopped	Manual	Enable	Enable	Enable
Workstation	Running	Auto		Disable if not used	Disable
World Wide Web Publishing Service	Running	Auto	Disable or remove	Disable if not used	Disable or remove