1 Security baseline for Windows 2003 Server

This document describes the steps necessary to harden an already installed Windows 2003 Server installation. Therefore it will not go into detail about the installation process. For each step that you do not follow in this guide, you should document why you didn’t. This document should then be added to the server’s documentation. It has been successfully tested on a few Windows 2008 server installations as well, but not enough that we want to call this a 2003/2008 guide.

Example:

If you choose not to do a clean installation of Windows 2003, put a mark (X) in the uppermost left portion of the item and document the reason for this action.

X	**Installation shall be done on a clean system**
Reason:	
When you upgrade a system, you will get a lot of extra files, leftover registry entries and other remaining data that could affect stability and security.	
Reason not to:	
Software couldn’t be installed directly onto the new system. We had to upgrade from Windows Server 2000.	

2 Checklist

Go through this checklist and document every time when you choose not to adhere to the baseline.

	Installation shall be done on a clean system
Reason:	

When you upgrade a system, you will get a lot of extra files, leftover registry entries and other remaining data that could affect stability and security.

Reason not to:

Only one Operating System on the server

Reason:

Avoid dual boot configurations. Otherwise, it may be trivial to boot into the other installation and bypass security settings on the first.

Reason not to:

English version must be used

Reason:

Localized Service Packs and software are released later than the native English one.

Reason not to:

	All partitions use NTFS
Reason:	
NTFS supports security properties and auditing. FAT16/32 does not.	
Reason not to:	

	The system must be installed on it’s own volume
Reason:	
In order to mitigate the risk of directory traversal attacks, the data must reside on another partition than the system. For more information on how Servers needs to be partitioned, see “ Baseline for Windows 2003 Server.doc”	
Reason not to:	

Attack surface must be reduced

Reason:

In order to mitigate the risk of compromise, you should only install the components explicitly requested by the customer.

Services that you should not be used by default:

Help and Support
IPSEC Services
Print Spooler
Windows Firewall/Internet Connection Sharing (ICS)
Wireless Configuration

(Some of those services can be needed. If you need to print from this server or print over this server, the print spooler must be running) Please note any other service that you chose to run / not to run under “Reason not to:” hereunder.

Reason not to:

No extra components

Reason:

Unless needed, no extra components should be installed by Add/Remove programs. If you need to install e.g. IIS, then note it under “Reason not to:” hereunder. A complete list of components that should be installed on ALL baseline servers can be found in “ Baseline for Windows 2003 Serverd.doc”

Reason not to:

Latest Service Packs added

Reason:

Unless warranted, the server should run the latest service packs available. The primary reason is security, but there is also the issue that installations may not be supported by Microsoft unless they are at a recently current Service Pack level.

The most current Service Pack levels can be found here:
http://www.microsoft.com/windows/lifecycle/servicepacks.mspx

Reason not to:

Lock down the filesystem

Reason:

Note: %SystemRoot% is the directory that holds the currently running installation of Windows. Normally it is c:\windows.

Remove "Everyone" and "All Users" from the root of the System disk.

Change the permissions on %SystemRoot%\repair and set that only Administrators and Systems have access (full access).

Create a new directory that only Administrators and SYSTEM have full access to called %SystemRoot%\dump. Enable auditing for Everyone on this folder and check all checkboxes under Failed and the “Change Permissions” checkbox under Successful.

Then goto the Control Panel - System - Advanced - Startup and Recovery settings. Change the path at “Dump File” to %SystemRoot%\dump\MEMORY.DMP. (It must end with a filename.)

Then run drwtsn32.exe and change the path ”Crash Dump” to %SystemRoot%\dump\user.dmp.

Reason not to:

Lock down the registry

Reason:

Disable AutoRun for CD-ROM drives.

Find this key key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CDRom\AutoRun
Change the value to : 0 (REG_DWORD)

Secure registry keys for the SNMP service.

Only allow these accounts to access the keys:
Administrators – Full Control
System – Full Control

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities

Secure the registry keys below with this access:

Administrators and System - Full Control

Authenticated Users – Read

Also set auditing for Everyone on these keys; check all checkboxes under Failed and the “Set Value” checkbox under Successful.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall
HKEY_LOCAL_MACHINE\Software\Microsoft\DrWatson (Leave the permissions for Terminal Server User, if exists)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
Select "winreg". Click Security and then click Permissions. Only those system, administrators and backup operators should have permissions. This is setup like this default on a Windows 2003 Server, but it’s worth checking this out anyway.

Navigate to Start / Control Panel / Administrative Tools / Local Security Policy”. Expand “Security Settings” and “Local Policies”. Choose "Security Options” and set ”Network security: Do not store LAN Manager hash value on next password change” to Enabled.

Reason not to:

Other settings that must be checked

Reason:

Load ”Event viewer” into the MMC. Right click on each log and choose ”Properties”. Set the following values:

Application Log: 16384 kb / Overwrite events as needed
Security Log: 16384 kb / Overwrite events as needed
System Log: 16384 kb / Overwrite events as needed

Navigate to Start / Control Panel / Administrative Tools / Local Security Policy”. Expand “Security Settings” and “Local Policies”. Choose "Security Options”, “Local Policy” and “Auditing Policy”. Set it up as follows:

Audit Account Logon events	Success, Failure
Audit Account Management	Success, Failure
Audit Logon Events	Success, Failure
Audit Object Access	Failure
Audit Policy Change	Success, Failure
Audit Privilege Use	Failure
Audit System Events	Success, Failure

Reason not to:

IIS if used must be locked down

Reason:

IIS must only be installed when needed. By default it is not installed with Windows 2003 server, and it's recommended that you carefully review what features you really need before installing the IIS role. All features that you do not need must be unchecked when you install the IIS role.

The inetpub-directory must be moved from the boot drive (normally c:\) to d:\. The easy way to do this is to move the directory and the change the document path for the site in IIS Admin. Remember to run "IISReset" afterwards to activated the new settings.

All administrative scripts must be removed from under the inetpub directory.

Stop the default site unless you really intend to use it.

All sites must be configured only to listen on the primary network connection. This is easy to achieve by using IIS Admin and choosing properties for the site in question. Under the tab named "Web Site" change "IP Address" from "(All Unassigned)" to the IP for the production LAN.

Always setup valid "host headers" for every site. The web server should not respond to requests that do not specify a valid DNS host header. This setting can be modified by running IIS Admin and choosing properties for the site in question. Under the tab named "Web Site" click "Advanced…" and configure the site correctly.

Review the authentication settings for each site. Remember that “Basic Authentication” is very easy to sniff for passwords. Avoid using it unless you do it on a secure (https) site. Integrated authentication is preferable for a site on the intranet, whereas Anonymous Authentication is allows anyone to see the pages. Digest authentication requires that you store the passwords with reversible encryption. It is best to avoid.

For extra hardening e.g. on a DMZ, consider installing URLScan and put the http method “TRACE” on the Deny list. If you know exactly what http methods that are to be used, you can configure URLSCAN only to allow those. But this can cause trouble with the function of the site if more functions are needed later on.

Never install the Frontpage extension on any site. They’re insecure by design and can open up serious vulnerabilities.

Reason not to: