



# Hardening WindowsNT

## Compass Security

### V0.96

### June 10<sup>th</sup>, 2002

Document name:	Hardening_WindowsNT_CSNC_V0.96.pdf
Version:	V0.96
Author:	Christoph Schnidrig, Compass Security AG <a href="mailto:christoph.schnidrig@csnc.ch">christoph.schnidrig@csnc.ch</a> <a href="http://www.csnc.ch">http://www.csnc.ch</a>
References:	a couple of other hardening doc / experience
Date of delivery:	June 10, 2002
Document state:	PUBLIC

GLÄRNISCHSTR. 7  
POSTFACH 1671  
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60  
Fax +41 55-214 41 61  
info@csnc.ch www.csnc.ch



## CONTENT

<b>1</b>	<b>INTRODUCTION.....</b>	<b>3</b>
1.1	<i>Version control</i>	4
1.2	<i>Local - Network - Application Security</i>	5
<b>2</b>	<b>HARDENING WINDOWS NT 4.0.....</b>	<b>7</b>
2.1	<i>How to read the table</i>	7
2.2	<i>Installation</i>	8
2.3	<i>System</i>	9
2.4	<i>User Management</i>	13
2.5	<i>Services included by WindowsNT</i>	17
2.6	<i>Secure Network Settings</i>	20
2.7	<i>Administering</i>	25
2.8	<i>File/Registry Permissions</i>	27
2.9	<i>Logging and Monitoring</i>	29
2.10	<i>General</i>	31
<b>3</b>	<b>HARDENING INTERNET INFORMATION SERVER 4.0.....</b>	<b>32</b>
3.1	<i>How to read the table</i>	32
3.2	<i>Installation</i>	33
3.3	<i>Authentication, Encryption and protecting confidential data</i>	35
3.4	<i>File- and Object Permissions/Logging</i>	36
3.5	<i>Removing unused stuff and features</i>	38
3.6	<i>Miscellaneous</i>	42
3.7	<i>Patches</i>	43
3.8	<i>Tools from Microsoft</i>	44
3.8.1	<i>Lockdown Tool</i>	44
3.8.2	<i>URLScan</i>	44
<b>4</b>	<b>APPENDIX.....</b>	<b>45</b>
4.1	<i>Tools</i>	45
4.2	<i>Resources</i>	45
4.3	<i>Utilities</i>	46
4.4	<i>Security Related Hotfixes after SP6a</i>	47
4.5	<i>How to find Security Fixes</i>	49
4.5.1	<i>Microsoft Network Security Hotfix Checker (HFNetChk)</i>	49
4.5.2	<i>Microsoft Download Center</i>	49
4.6	<i>Portlist</i>	49
4.7	<i>Compass Script</i>	50



## **1 Introduction**

This document describes how to harden a WindowsNT box in order to gain more security according to the aspect of

- Network security
- Local security

Compass is working on this paper. If you found some bugs, feel free to send an e-mail. Comments and inputs are appreciated as well. I will leave the version control chapter in the future. So everybody can see who did what on this document.



## 1.1 Version control

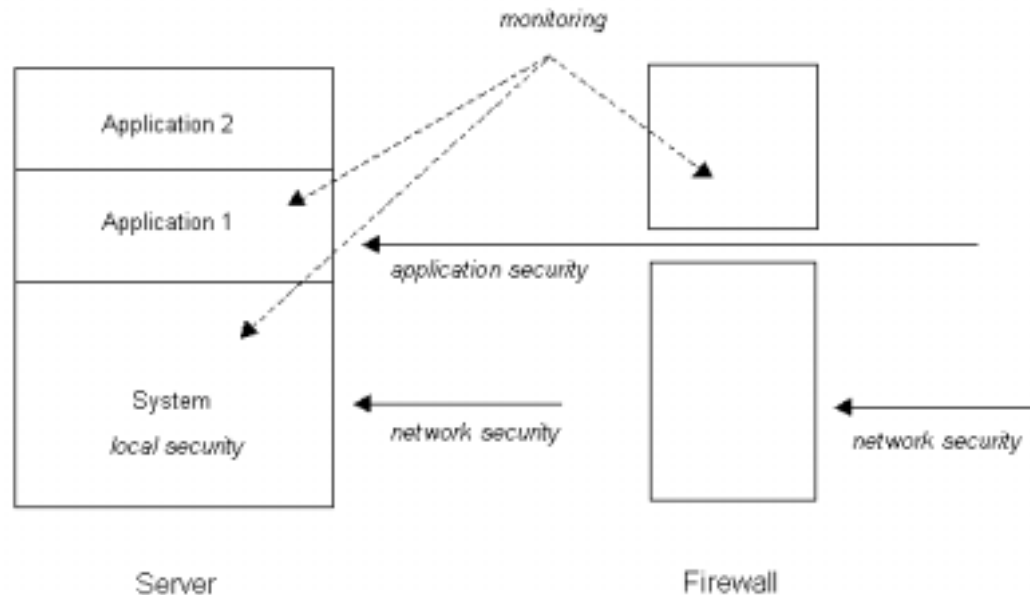
Version	Author	Description	Filename
0.80	Christoph Schnidrig <a href="mailto:christoph.schnidrig@csnc.ch">christoph.schnidrig@csnc.ch</a>	Initial version saved on <a href="http://www.csnc.ch/download">http://www.csnc.ch/download</a>	Hardening_WindowsNT_CSNC_V0.80.pdf
0.81	Christoph Schnidrig	Some minor changes, Add some notes.	Hardening_WindowsNT_CSNC_V0.81.pdf
0.90	Christoph Schnidrig	Include a new Chapter about IIS 4.0 Hardening. Fix the Link to the Scripts. Add Chapter 4.4. Improve the Service Desc.	Hardening_WindowsNT_CSNC_V0.90.pdf
0.91	Ivan Bütler Christoph Schnidrig	Review Updated Hotfixes see 4.4	Hardening_WindowsNT_CSNC_V0.91.pdf
0.95	Christoph Schnidrig	General Update Script Update	Hardening_WindowsNT_CSNC_V0.95.pdf
0.96	Christoph Schnidrig	Updated Hotfixes see 4.4 Addition to Chapter 3.8.2	Hardening_WindowsNT_CSNC_V0.96.pdf

## 1.2 Local - Network - Application Security

Compass defined 3 levels of hardening tasks

local security hardening	[threat to local exploits]
network security hardening	[threat to LISTEN services - remote exploits]
application security hardening	[threat to application]
monitoring tasks	[attack detection / alarming and alerting]

All LISTEN services not used for the application (e.g. telnet) is discussed as network security aspect.



### Hardening an application can be:

- Limiting user rights
- Limiting rights of process owner
- Checking file permissions of application specific files
- Restricting access to other system resources

If an application is exploitable, the attacker should find a very unfriendly environment. That means it should be difficult for him to break the system or to attack other systems.

### Hardening on network security level means:

- Use secure protocols for administration
- Disable unused network services
- Disable trust relations to other systems
- Disable unused accounts
- Enforce strong passwords
- Disable dangerous network services
- Restrict access to the required systems, persons

### Hardening on local security level means:

- Restrict access to powerful commands
- Set correct file permissions
- Apply group and user concept
- Disable unused services



Eventually people are aware in take advantage of firewall infrastructure before proceeding with e-business applications. But whatever you do to protect your DMZ hosts by a firewall, the application port need to be open for the outside world. That's why you have e-business! With this in mind, we defined the following hacking scenario:

- Hacker exploits the offered e-business application. In most cases by SSL, HTTP or IIOP (Corba). Let's assume the worst case, the hacker gains an interactive connection to this application by a shell.
- Most customers have three tier architecture. It might be needed (in the eyes of an attacker) to gain more privileges on the system, in order to read include files from the application (database definitions) or to set the network interface in promiscuous mode (sniffing the DMZ-LAN). The worst case in such a scenario would be, that the attacker gains "root" or administrative privileges
- After the e-business tier is under full control of the hacker, he or she might want to access confidential data on a nearby database system. The hacker has fully access to all LISTEN or Idle services (not only to the application port, if we assume the DB belongs to the same DMZ segment).

You might ask yourself, why I did not write a "Hardening E-Business application" article, because this seems to be the first step a hacker has to take. You are right. I strongly believe in application security aspects. But various e-business applications are available out there and the hardening depends from application to application. Please checkout the hardening Apache or Hardening WebSphere checklist. The latest article can be downloaded from our website, because we already helped clients in hardening WebSphere. Hardening Apache Checklists are available at [www.apache.org](http://www.apache.org) and more Microsoft Checklists are available at [www.microsoft.com/security](http://www.microsoft.com/security).

If you read this article, please keep in mind the hardening tasks below described in the task list table only protect step 2 and step 3 of the hacking scenario above. We want to make sure, the hacker can't easily gain more privileges on your system and if you expect another DMZ host being hacked not being an easy hacking target. Don't trust your other DMZ hosts!!! This article might help you to define your security policy, before new Windows NT machines are rolled out in the Intra\_NET.



## 2 Hardening Windows NT 4.0

### 2.1 How to read the table

H = Hardening

L = Task influences local security aspects

N = Task influences network security aspects

No.	Description	How to fix	H		Reference
number	short brief description of the problem	discussion how to fix the problem	L	N	what script might automate this task

You will find scripts in the end of this article. During the hardening procedure this scripts is called Compass-Script. This script includes some of my conclusion about the necessary hardening steps. All other are defined in the reference row as “to do by Hand”. So it is your decision to do the individual steps automatically or by hand.

I’ve defined the “Must”-Steps with an asterisk (\*) after the number. These steps are my opinion to get a minimum Security-Level for a DMZ-System. This should be a little help but the decision is yours.



## 2.2 Installation

#	Installation	How to fox	L	N	Reference
1001*	Install available hotfixes	<p>Install all available hotfixes. The hotfixes are available from <a href="ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40">ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40</a></p> <p>Check also the Microsoft Download Center Search Engine at <a href="http://www.microsoft.com/downloads/search.asp">http://www.microsoft.com/downloads/search.asp</a>.</p> <p>To Check Versions of Installed Hotfixes see KBase Q238552, check HKLM\Software\Microsoft\Windows NT\CurrentVersion\Hotfix, run winver.or get the Network Security Hotfix Checker Tool from MS. See chapter 4.4 and 4.5 in this document.</p>	X		to do by hand
1002	Remove additional OS installations	Whenever possible, remove any additional Linux, OS/2, or other OS installations. If you have additional Windows NT installations for disaster recovery, make sure it's secured according to the steps in this checklist.	X		to do by hand
1003*	Format all Partitions with NTFS	<p>Format all Disks with NTFS, this will enable the ACL on Filelevel.</p> <p>To convert a FAT-Formatted Disk type: <code>CONVERT drive: /FS:NTFS</code></p>	X		to do by Hand
1004*	Remove Client Software from Server	Remove all Client Software like Outlook, Outlook Express, Word, Media Player... from Server. If you really need a browser on the server, use Netscape instead Internet Explorer. There are many Exploits for IE (e.g. Active X-Stuff). Try to avoid using a server as a "client", because major risks arise by inside-out attacks	X		to do by Hand



## 2.3 System

#	System	How to fix	L	N	Reference
2001*	Disable CDROM Auto-Run	Prevents malicious auto-run programs to be invisible or appear benign  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Sevices\Cdrom\Autorun  Set its value to 0 to disable auto-run. (See KBase Q155217 and Q126309.). It's might important, if the hacker potentially a malicious cdrom into the server. (but by the way...there are other more efficient ways to hack a system when physical access is possible.	X		to do by Compass-Script
2002*	Ensure only the interactive user can access floppy drives.	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon  Add/change a REG_SZ-Value named AllocateFloppies with a 1 in it.  Note: By default allows NT access all user to FD. FD uses also FAT, so there are no file permissions. Not an issue, if system is physically protected.	X		to do by Compass-Script
2003*	Ensure only the interactive user can access CD-ROM drives.	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon  Add/change a REG_SZ-Value named AllocateCdRoms with a 1 in it.  Not an issue, if system is physically protected.	X		to do by Compass-Script
2004	Disabling the Registry Editors	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System  If this Registry key has a value named "DisableRegistryTools" with a REG_DWORD value of 1, the standard Registry editing tools do not run.	X		to be done by hand



#	System	How to fix	L	N	Reference
2005*	Shutting Down the System without logon	<p>If the Registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon has a value named "ShutdownWithoutLogon" with a REG_SZ value of "1," then a "Shutdown" button appears on the logon window that allows anyone to shut the system down without logging on.</p> <p>Note: It is already disabled by Windows NT Server but not by Workstation! Not an issue, if system is physically protected.</p>	X		to do by Compass-Script
2006*	Remove POSIX and OS/2 subsystems	<p>Delete \winnt\system32\os2 directory and all subdirectories</p> <p>Delete the OS2.EXE, OS2SS.EXE, OS2SRV.EXE, PSXSS.EXE, PSXDLL.DLL, POSIX.EXE files from \winnt\system32</p> <p>Delete HKLM\SOFTWARE\Microsoft\OS/2 Subsystem for NT and all subkeys</p> <p>Delete HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\Os2LibPath key value</p> <p>HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems Delete OS2 and Posix key values Delete OS2 and Posix from Optional values</p> <p>Note: This subsystems are not C2 approved and commonly unneeded!</p>	X		to do by Compass-Script
2007*	Remove other potential dangerous tools  (we recommend to copy this tools to a cdrom and include the cdrom into PATH for the admin account. Insert the cdrom only, if needed. This	<p>arp.exe, at.exe, atsvc.exe, cacls.exe, cmd.exe, cscript.exe, debug.exe, edit.com, edlin.exe, finger.exe, ftp.exe, ipconfig.exe, nbtstat.exe, net.exe, netstat.exe, nslookup.exe, ping.exe, qbasic.exe, rcp.exe, rdisk.exe, regedit.exe, regedt32.exe, rexec.exe, route.exe, rsh.exe, runonce.exe, secfixup.exe, syskey.exe, telnet.exe, tftp.exe, tracert.exe, wscript.exe, xcopy.exe</p> <p>Move and ACL Critical Files: Remove the following files from the system32 directory and copy them to an admin-created directory, AND ACL the files.</p>	X		to do by Compass-Script



#	System	How to fix	L	N	Reference
	task would reject all known UNICODE exploits from the past, because the cmd.exe would not been accessible by the IIS daemon.	and copy them to an admin-created directory, AND ACL the files.			
2008*	Wiping the System Page File during clean system shutdown	You may want to ensure that system page file is wiped clean when WindowsNT shuts down. This ensures that sensitive information from process memory that may have made into the page file is not available to a snooping user. This can be achieved by setting up the following key:  HKEY_LOCAL_MACHINE\SYSTEM\System\CurrentControlSet\Control\SessionManager\Memory Management\ClearPageFileAtShutdown (=1 REG_DWORD)	X		to do by Compass-Script
2009	Disable caching of logon information	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon  Add/change a REG_SZ-Value named CachedLogonsCount with a 0 in it.  For RAS-Access also in:  HKLM\System\CurrentControlSet\Services\Rasman\Parameters]  Add/change a DWORD-Value named DisableSavePassword with a 1 in it. See KBASE and give a search to “Where NT stores passwords”	X		to do by Hand
2010	Turn off NTFS 8.3 Name Generation	To turn off 8.3 name generation set the following registry entry:  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\  Add/Change a REG_DWORD-Value named NtfsDisable8dot3NameCreation with a 1 in it.	X		to do by Hand



#	System	How to fix	L	N	Reference
		Note: In a secure Environment it is important to avoid using 16bit Apps. So this stuff is unneeded. There are also performance issues, the can be 10-15% slower with 8.3 Name Generation enabled.			
2011	System boot time set to zero seconds	Go to Control Panel-System-Startup/Shutdown and set „Show list for“ to zero.  Not an issue, if system is physically protected.	X		to do by Hand
2012	Remove the Clipboard Viewer	The Clipbook viewer is not included in the evaluation of Windows NT, and therefore must be removed. To do this, go to Control Panel-Add/Remove Software-Windows NT Setup-Accessoires-Clipboard Viewer and uncheck the box.	X		to do by Hand
2013*	Do not move files to the Recycle Bin. Delete files	Select the “Do not move files to the Recycle Bin” option of the recycle bin properties sheet to ensure that on deletion files are permanently removed from the system.	X		to do by Hand
2014*	Secure base objects	To enable stronger protection on base objects, add the following value to the registry key  HKLM\SYSTEM\CurrentControlSet\Control\Session Manager  Add/change a REG_DWORD-Value named ProtectionMode with a 1 in it.  Among other things, it prevents users from gaining local administrator privileges by way of a dynamic-link library (DLL). This issue is explained in more detail here <a href="http://www.microsoft.com/technet/security/bulletin/ms99-006.asp">http://www.microsoft.com/technet/security/bulletin/ms99-006.asp</a>	X		to do by Compass-Script



## 2.4 User Management

#	User Management	How to fix	L	N	Reference
3001	Displaying a Legal Notice Before Log On	<p>Windows NT can display a message box with the caption and text of your choice before a user logs on. To display a legal notice, use the Registry Editor to create or assign the following registry key values on the workstation to be protected:</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\LegalNoticeCaption</p> <p>Add an REG_SZ-Value with the legal notice you like.</p>	X		to do by hand
3002*	Hiding the Last User Logon	<p>By default, Windows NT displays the previous account name on the logon window. You can prevent this by creating a value named "DontDisplayLastUserName" with a REG_SZ value of "1" in the Registry key:</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon</p>	X		to do by Compass-Script
3003*	Password policy:	<p>Enforce password uniqueness by remembering last passwords 6            Minimum password age: 2            Maximum password age: 42            Minimum password length: 8            User must logon to change password: Enabled            Account lockout policy Account lockout count: 5            Lockout account time: forever            Reset lockout count after: 720 minutes            Complex passwords (passfilt.dll): Enabled</p> <p>To Enable strong password functionality with passfilt.dll see KBase Q161990</p>		X	to do by Hand



#	User Management	How to fix	L	N	Reference																				
3004*	Make sure the Guest account is disabled	By default, the Guest account is enabled on Windows NT Workstation systems. If the Guest account is enabled, disable it.		X	to do by Hand																				
3005*	Rename Administrator account	Rename the Administrator Account. It is also a good idea create a low-privileged account called administrator and enable the logging for failed logons. In this case you can see if a hacker tries to logon as administrator ;-) [honey pot]  Note, that nbtstat -a or nbtstat -A may be used to determine the real administrator account if they are currently logged on.		X	to do by Hand																				
3006*	Verify that the Administrator account has a strong password	Windows NT allows passwords of up to 14 characters. In general, longer passwords are stronger than shorter ones, and passwords with several character types (letters, numbers, punctuation marks, and non-printing ASCII characters, generated by using the Alt key and three-digit key codes on the numeric keypad) are stronger than alphabetic or alphanumeric-only passwords.		X	to do by Hand																				
3007*	Modify user rights membership	Use User Manager for Domains to restrict the use of user rights as shown in Table.  <table border="1"> <thead> <tr> <th>User Right</th> <th>Membership</th> </tr> </thead> <tbody> <tr> <td>Access this computer from network</td> <td>Trusted users who need remote access</td> </tr> <tr> <td>Act as part of the operating system</td> <td><b>Do not assign to any user.</b></td> </tr> <tr> <td>Add workstations to domain</td> <td>Domain Admins</td> </tr> <tr> <td>Back up files and directories</td> <td>trusted users (e.g. the Backup Operators group)</td> </tr> <tr> <td>Bypass traverse checking</td> <td>Authenticated Users</td> </tr> <tr> <td>Change the system time</td> <td>trusted users (e.g. Server Operators)</td> </tr> <tr> <td>Create a pagefile</td> <td>trusted users (e.g. Server Operators)</td> </tr> <tr> <td>Create a token object</td> <td><b>Do not assign to any user.</b></td> </tr> <tr> <td>Create permanent shared objects</td> <td>(no one)</td> </tr> </tbody> </table>	User Right	Membership	Access this computer from network	Trusted users who need remote access	Act as part of the operating system	<b>Do not assign to any user.</b>	Add workstations to domain	Domain Admins	Back up files and directories	trusted users (e.g. the Backup Operators group)	Bypass traverse checking	Authenticated Users	Change the system time	trusted users (e.g. Server Operators)	Create a pagefile	trusted users (e.g. Server Operators)	Create a token object	<b>Do not assign to any user.</b>	Create permanent shared objects	(no one)		X	to do by Hand
User Right	Membership																								
Access this computer from network	Trusted users who need remote access																								
Act as part of the operating system	<b>Do not assign to any user.</b>																								
Add workstations to domain	Domain Admins																								
Back up files and directories	trusted users (e.g. the Backup Operators group)																								
Bypass traverse checking	Authenticated Users																								
Change the system time	trusted users (e.g. Server Operators)																								
Create a pagefile	trusted users (e.g. Server Operators)																								
Create a token object	<b>Do not assign to any user.</b>																								
Create permanent shared objects	(no one)																								



#	User Management	How to fix	L	N	Reference
		Debug programs (no one) <b>This right is not auditable!</b> Force shutdown from a remote sys. trusted users (e.g. Server Operators) Generate security audits <b>Do not assign to any user.</b> Increase quotas trusted users (e.g. Server Operators) Increase scheduling priority trusted users (e.g. Server Operators) Load and unload device drivers trusted users (e.g. Server Operators) Lock pages in memory (no one) Log on as a batch job trusted users (as needed) Log on as a service trusted users (as needed) Log on locally Trusted users (as needed) Manage auditing and security log trusted users (e.g. Domain Admins) Modify firmware environment value trusted users (e.g. Domain Admins) Profile single process trusted users Profile system performance trusted users Replace a process level token <b>Do not assign to any user.</b> Restore files and directories trusted users (e.g. Backup Operators) Shut down the system trusted users (e.g. Server Operators) Take ownership of files or objects trusted users (e.g. Domain Admins)			
3008*	Encrypt the system accounts database	Run the <code>syskey.exe</code> utility (with the key on harddisk option). This will provide protection against password cracking tools like L0pht Crack ( <a href="http://www.l0pht.com/">http://www.l0pht.com/</a> ). This Tool is included since SP2.  See KBase Q143475.		X	to do by Hand
3009*	Set Screen Saver:	To protect the console of the server, set up the screen saver for the administrator's profile:	X		to do by Compass-Script



#	User Management	How to fix	L	N	Reference
		<p>Go to Display &gt; Screen Saver &gt; Logon Screen Saver and select Enable Password Protect. Click OK.</p> <p>Not an issue, if system is physically protected or no remote desktop software is used like PCAnywhere, PC Duo, VNC, ...</p>			
3010*	Enable network lockout of admin account.	<p>Use the NT Resource Kit's passprop utility to run the following command:  <code>passprop /adminlockout /complex</code></p> <p>You still able to log on interactive! Note: /complex is used for enable stronger passwords – see also # 3003.</p>		X	to do by Hand
3011*	Unauthenticated Event Log Viewing	<p>You can prevent this by creating a value named  “RestrictGuestAccess” with a REG_DWORD value of 1 in the Registry keys:  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Application  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\System</p>	X		to do by Compass-Script
3012*	Restrict the ability to add printer drivers	<p>“AddPrinterDrivers” with a REG_DWORD value of 1 in the Registry key:  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers</p> <p>Untrusted print drivers can maliciously divert user data.</p>	X		to do by Compass-Script
3013*	Prevent user from running Task Manager	<p>HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\System\  Add/Change a REG_DWORD-Value named DisableTaskMgr with a 1 in it.</p>	X		to do by Compass-Script

## 2.5 Services included by WindowsNT

#	Services included by NT	How to fix	L	H	Reference																				
4001*	<p>Disable as many as possible of the following services</p> <p>Note: You have to check which service is needed by your application or not! Check also this website <a href="http://arstechnica.com/tweak/nt/ntservices-1.html">http://arstechnica.com/tweak/nt/ntservices-1.html</a> ,it will also help to decide which service you really need.</p>	<p>Disable the following Services:</p> <table border="1"> <tr> <td>Alerter</td> <td>Send alert messages, such as disk full, to administrators. Depends upon the Messenger service</td> </tr> <tr> <td>ClipBook Server</td> <td>The ClipBook Server permits cutting and pasting over the network.</td> </tr> <tr> <td>Computer Browser</td> <td>Provides browsing capabilities that allow users to find resources on the network</td> </tr> <tr> <td>DHCP Client</td> <td>Provide dynamic IP configuration</td> </tr> <tr> <td>Directory Replicator</td> <td>Provides automated duplication of directories over NT based Computer.</td> </tr> <tr> <td>License Logging Service</td> <td>The service that logs the licensing data for License Manager</td> </tr> <tr> <td>Messenger</td> <td>Used to send network messages to Windows Network machines and users</td> </tr> <tr> <td>Net Logon</td> <td>Validates user account logon and synchronizes domain accounts. Only needed on Domain Controllers.</td> </tr> <tr> <td>Network DDE</td> <td>A form of interprocess communication (IPC) implemented in the Microsoft Windows family of operating systems. Two or more programs that support dynamic data exchange (DDE) can exchange information and commands</td> </tr> <tr> <td>Network DDE DSDM</td> <td>DDE share database manager service manages shared DDE conversations. It</td> </tr> </table>	Alerter	Send alert messages, such as disk full, to administrators. Depends upon the Messenger service	ClipBook Server	The ClipBook Server permits cutting and pasting over the network.	Computer Browser	Provides browsing capabilities that allow users to find resources on the network	DHCP Client	Provide dynamic IP configuration	Directory Replicator	Provides automated duplication of directories over NT based Computer.	License Logging Service	The service that logs the licensing data for License Manager	Messenger	Used to send network messages to Windows Network machines and users	Net Logon	Validates user account logon and synchronizes domain accounts. Only needed on Domain Controllers.	Network DDE	A form of interprocess communication (IPC) implemented in the Microsoft Windows family of operating systems. Two or more programs that support dynamic data exchange (DDE) can exchange information and commands	Network DDE DSDM	DDE share database manager service manages shared DDE conversations. It		X	to do by Hand
Alerter	Send alert messages, such as disk full, to administrators. Depends upon the Messenger service																								
ClipBook Server	The ClipBook Server permits cutting and pasting over the network.																								
Computer Browser	Provides browsing capabilities that allow users to find resources on the network																								
DHCP Client	Provide dynamic IP configuration																								
Directory Replicator	Provides automated duplication of directories over NT based Computer.																								
License Logging Service	The service that logs the licensing data for License Manager																								
Messenger	Used to send network messages to Windows Network machines and users																								
Net Logon	Validates user account logon and synchronizes domain accounts. Only needed on Domain Controllers.																								
Network DDE	A form of interprocess communication (IPC) implemented in the Microsoft Windows family of operating systems. Two or more programs that support dynamic data exchange (DDE) can exchange information and commands																								
Network DDE DSDM	DDE share database manager service manages shared DDE conversations. It																								



#	Services included by NT	How to fix	L	H	Reference
		is used by the Network DDE service			
	Plug an Play (needed for access the devices on control panel!)	A service that fudges <i>some</i> functionality of Plug and Play, standard in Windows 9x. For those of you having used unimodem modems in NT4, you should be quite familiar with this service (as it's needed to detect and use such modems). Other than that, we all know what PnP is.			
	Remote Procedure Call (RPC) Locator	The Remote Procedure Call Locator service allows distributed applications to use the RPC Name service. The RPC Locator service manages the RPC Name service database.			
	Scheduler	The <b>at</b> command can schedule commands and programs to run on a computer at a specified time and date.			
	Server	Provides RPC (remote procedure call) support, and file, print, and named pipe sharing.			
	Spooler	A process on a server in which print documents are stored on a disk until a printing device is ready to process them.			
	SNMP service	The agent processes SNMP Request messages that it receives from SNMP management systems			
	SNMP trap	Which listens for traps sent to the NT host and then passes the data along to			



#	Services included by NT	How to fix	L	H	Reference																		
		<table border="1"> <tr> <td></td> <td>the Microsoft SNMP management API</td> </tr> <tr> <td>TCPIP NetBIOS Helper</td> <td>NetBIOS</td> </tr> <tr> <td>Telephony Service</td> <td>RAS-Service</td> </tr> <tr> <td>UPS</td> <td>Manages an uninterruptible power supply connected to a computer.</td> </tr> <tr> <td>Workstation</td> <td>Provides network connections and communications.</td> </tr> </table> <p>This services you need:</p> <table border="1"> <tr> <td>EventLog</td> <td>Records events in the system, security, and application logs.</td> </tr> <tr> <td>NT LM Security Support Provider</td> <td>The RPC subsystem includes the endpoint mapper and other miscellaneous RPC services.</td> </tr> <tr> <td>Remote Procedure Call (RPC) Service</td> <td>The RPC subsystem includes the endpoint mapper and other miscellaneous RPC services.</td> </tr> <tr> <td></td> <td></td> </tr> </table>		the Microsoft SNMP management API	TCPIP NetBIOS Helper	NetBIOS	Telephony Service	RAS-Service	UPS	Manages an uninterruptible power supply connected to a computer.	Workstation	Provides network connections and communications.	EventLog	Records events in the system, security, and application logs.	NT LM Security Support Provider	The RPC subsystem includes the endpoint mapper and other miscellaneous RPC services.	Remote Procedure Call (RPC) Service	The RPC subsystem includes the endpoint mapper and other miscellaneous RPC services.					
	the Microsoft SNMP management API																						
TCPIP NetBIOS Helper	NetBIOS																						
Telephony Service	RAS-Service																						
UPS	Manages an uninterruptible power supply connected to a computer.																						
Workstation	Provides network connections and communications.																						
EventLog	Records events in the system, security, and application logs.																						
NT LM Security Support Provider	The RPC subsystem includes the endpoint mapper and other miscellaneous RPC services.																						
Remote Procedure Call (RPC) Service	The RPC subsystem includes the endpoint mapper and other miscellaneous RPC services.																						
4002*	If you need the SNMP-Service – set an unpredictable Community String	Go to Control Panel-Network-Services-SNMP Service-Properties-Security-Accepted Community Names. Select Public community name and click on Edit. Enter [YOUR COMMUNITY STRING] <b>Note:</b> Set a strong password Click [OK] to accept changes. Click [OK] to close the MS SNMP Properties		X	to do by Hand																		
4003*	Change the Scheduler service's security context (if the scheduler is needed)	The context in which a system service runs determines what it can do. By default, the Schedule service runs in the LocalSystem context, meaning that users may be able to schedule jobs that run in a context that exceeds their own permission level. To change the security context for the Scheduler service, do the following:		X	to do by Hand																		



#	Services included by NT	How to fix	L	H	Reference
		<ul style="list-style-type: none"> <li>Open the Services control panel (Start   Settings   Control Panel   Services).</li> <li>Select the Schedule service, then click the Startup button. The Service information dialog will appear.</li> <li>In the Log On As group, select the "This account" radio button. Enter a set of account credentials for the service to use, then click the OK button.</li> <li>Stop and restart the service.</li> </ul>			

## 2.6 Secure Network Settings

#	Network	How to fix	L	N	Reference
5001*	Ensure that TCP/IP is the only protocol installed:	In the Network Control Panel under the Protocols tab, remove all except for TCP.		X	to do by Hand
5002	Restricting who can Access the Registry Remotely	<p>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\WINREG</p> <p>If this Registry key exists then only users listed in its ACL, or who belong to groups listed in its ACL, can access the Registry remotely. Use regedt32.exe and mark the Key you want ACL and go to Security-Permission.</p>		X	to do by Hand
5003*	Restrict anonymous users from being able to obtain public LSA information	Windows NT allows users who, by virtue of the trust relationships, have no access to certain domains to nonetheless see user account names, as well as network and printer share names on computers in those domains. To prevent this anonymous viewing of names, one can add a value named "RestrictAnonymous" with a REG_DWORD value of 1 to the key:		X	to do by Compass-Script



#	Network	How to fix	L	N	Reference
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa			
5004*	Restrict Null Session Access over Named Pipes	HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters  Remove all entries from the following two key values: NullSessionPipes and NullSessionShares		X	to do by Compass-Script
5005*	Disable NETBIOS  (Use SSH for filehandling)	By unbinding the WINS Client in the Network application from all adapters, we get rid of all listeners on the NETBIOS ports. Network -> Bindings -> All protocols -> WINS Client -> Disable. Also disable the WINS Client driver in Control Panel -> Devices -> WINS Client -> Disable. Note: These operations include directory and printer sharing, NetDDE (network Dynamic Data Exchange), and remote administration.		X	to do by Hand
5006	Configure TCP/IP filters  Skip this step if you are to install another packet filtering software on this host later on.	Configure TCP/IP-security by specifying the ports that are allowed inbound (TCP or UDP) on each network adapter. This is done in the Network application-Protocol-TCP/IP-Advanced-Enable Security-Configure.  Example: Web-Server The configuration shown to the right allows only connections to tcp/80. No UDP is accepted. IP protocol 6 is TCP.  See for a Port-List <a href="http://www.isi.edu/in-notes/iana/assignments/port-numbers">http://www.isi.edu/in-notes/iana/assignments/port-numbers</a>		X	to do by Hand
5007*	Remove "hidden" administrative shares  Like c\$, admin\$...	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters  Add/Change the DWORD-Value AutoShareServer (Server) with a 0 in it.  Add/Change the DWORD-Value AutoShareWks (Workstation) with a 0 in it.		X	to do by Compass-Script
5008	Unencrypted Passwords on the Network	Windows NT has the ability to communicate with certain non-Windows NT systems that require sending user passwords unencrypted ("plaintext") over the network. This feature is disabled by default and must be manually enabled by adding the value		X	



#	Network	How to fix	L	N	Reference
		<p>named</p> <p>“EnablePlainTextPassword” with a REG_DWORD value of 1 to the Registry key:</p> <p>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RDR\Parameters</p> <p>Prevent Windows NT from passing unencrypted passwords across the network by removing the EnablePlainTextPassword value from this Registry key. This feature was implemented in Windows NT 4.0 SP3. See also [KBase] Q166730.</p>			
5009	<p>Configure Server Message Block authentication protocol</p> <p>(only if NetBIOS is enabled!)</p>	<p>Require SMB signing of server and/or client activities by creating REG_DWORD values named “EnableSecuritySignature” and “RequireSecuritySignature” with a value of 1 in the following Registry keys:</p> <p>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters</p> <p>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rdr\Parameters</p> <p>This feature was implemented in 4.0 SP3. See KBase Q161372, “How to Enable SMB Signing in Windows NT”. Note: This feature has to be enabled on all systems!</p>		X	to do by Hand
5010*	Prevent using LANMAN Passwords	<p>To prevent Windows NT from using the LANMAN format, create and set the REG_DWORD value named “LMCompatibilityLevel” in the Registry key:</p> <p>HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\LSA</p> <p>0 – Send both NT and LM            1 – Send what are requested            2- Send only NT (Win95 will not able to connect!)</p> <p>This feature was implemented in 4.0 SP3. See KBase Q147706</p>		X	to do by Compass-Script



#	Network	How to fix	L	N	Reference
5011	DCOM RPC high ports	<p>By default DCOM dynamically allocates one high port (&gt;1023) per process. There is a way to limit the portmapper to only a specific range of ports. You must decide how many ports you want to allocate, which is equivalent to the number of simultaneous DCOM processes through the firewall. You must open all of the UDP and TCP ports corresponding to the port numbers you choose. In addition, you must open TCP/UDP 135, which is used for RPC End Point Mapping, among other things. In addition, you must tell DCOM which ports you reserved using the following registry key:</p> <p>HKEY_LOCAL_MACHINES\Software\Microsoft\Rpc\Internet</p> <p>You probably will have to create this key. Here is an example of how to restrict DCOM to a range of 10 ports:</p> <p>Named value: Ports Type: REG_MULTI_SZ Setting: Range of port. Can be multiple lines such as: 3001-3010 135.</p> <p>Named value: PortsInternetAvailable Type: REG_MULTI_SZ Setting: "Y"</p> <p>Named value: UseInternetPorts Type: REG_MULTI_SZ Setting: "Y"</p>		X	to do by Hand
5012	Set NTLM security to response only	<p>\HKLM\SYSTEM\CurrentControlSet\Control\LSA Add/change key value: <b>LMCompatibilityLevel</b> data type: REG_DWORD value: 2</p> <p>\HKLM\SYSTEM\CurrentControlSet\Control\LSA\MSV1_0 Add/change key value: <b>NtLmMinClientSec</b> data type: REG_DWORD</p>		X	

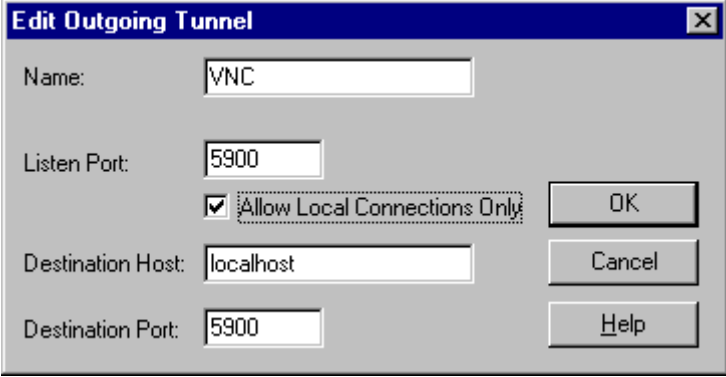
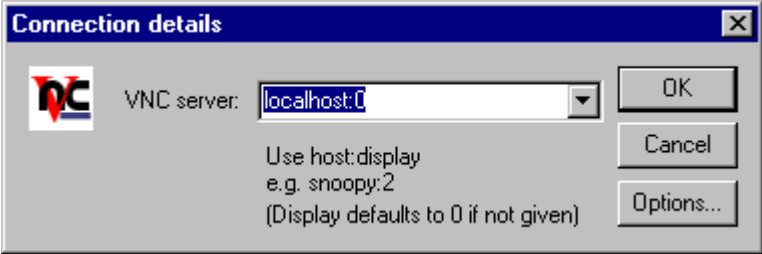


#	Network	How to fix	L	N	Reference
		value: 0 Add/change key value: <b>NtlmMinServerSec</b> data type: REG_DWORD value: 0 See KBase Q147706.			



## 2.7 Administering

#	Administering	How to fix	L	N	Reference	
6001	<p>Setting up secure Administrating with SSH and VNC</p> <p><b>Note:</b> If you move cmd.exe from /winnt/system32 the SSH-Server will not start! The Compass-Script will also move the cmd.exe! You have to move it back, if you like run the SSH-Server!</p>	<p><b>Used Software:</b>            SSH-Server (30Day Testversion):  <a href="http://ftp.ssh.com/pub/ssh/SSHWinServer.exe">http://ftp.ssh.com/pub/ssh/SSHWinServer.exe</a>            SSH Client (non-commercial):  <a href="http://ftp.ssh.com/pub/ssh/SSHWin-2.4.0-pl2.exe">http://ftp.ssh.com/pub/ssh/SSHWin-2.4.0-pl2.exe</a>            VNC:  <a href="http://www.uk.research.att.com/vnc/dist/vnc-3.3.3r9_x86_win32.zip">http://www.uk.research.att.com/vnc/dist/vnc-3.3.3r9_x86_win32.zip</a></p> <p><b>Installation Steps on the server machine:</b>            Install and start the VNC-Server. For more information about VNC have a look at:  <a href="http://www.uk.research.att.com/vnc/">http://www.uk.research.att.com/vnc/</a></p> <p>Use regedit, add the DWROD value AllowLoopback=1 to HKLM\SOFTWARE\ORL\WinVNC3.</p> <p>Install and set up SSH-Server.</p> <p>Make sure you're running SSH-Server and WinVNC on the target machine.</p> <p><b>Installation Steps on the client machine:</b></p> <p>Install the SSH-Client</p> <p>Unpack the VNC-Client (vncviewer.exe)</p> <p>Start up the SSH-Client and setup the SSH-Tunnel:            Go to Edit-Settings-Host Settings-Tunneling-Outgoing and Click add</p>			X	to do by Hand

#	Administering	How to fix	L	N	Reference
		 <p>Connect with the SSH-Client to the server machine. The Tunnel will set up automatically.</p> <p>Start up the VNC-Viewer:</p>  <p>Type localhost:0 in – and OK... ...Voila VNC over SSH ☺</p> <p>It's a good idea to use IP-Filtering to restrict access on the server!</p>			



## 2.8 File/Registry Permissions

#	File/Registry Permissions	How to fix	L	N	Reference
7001	Lock down "Users":	<p>Recursively set permissions for the built-in NT group "Users" to "No Access" for all volumes:</p> <p>- Since a newly created user is automatically added to the "Users" group, new users, by default, will not have access to any information on any of the volumes.</p>		X	to do by Hand
7002*	Restrict untrusted users from being able to plant trojan horse programs in these locations	<p>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run            HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall (if present)            HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce            HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AEDebug</p> <p>Change the access control entry for Everyone in the above Registry keys and all subkeys to Read. Do not modify any other access control entries. Use regedt32.exe.</p>		X	to do by Hand
7003	Only Administrators can create shares	<p>HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares</p> <p>Set the following permissions on the above key and all subkeys:</p> <p>Administrators Full Control            SYSTEM Full Control            Everyone Read</p>		X	to do by Hand
7004	Disable direct draw	<p>This prevents direct access to video hardware and memory.</p> <p>\HKLM\SYSTEM\CurrentControlSet\Control\GraphicsDrivers\DCI</p> <p>Add/change key value: <b>Timeout</b>            data type: REG_DWORD</p>	X		to do by Hand



#	File/Registry Permissions	How to fix	L	N	Reference
		value: 0			
7005*	Protecting Files and Directories	<p>Among the files and directories to be protected are those that make up the operating system software itself. The standard set of permissions on system files and directories provide a reasonable degree of security without interfering with the computer's usability. For high-level security installations, however, you might want to additionally set directory permissions to all subdirectories and existing files immediately after Windows NT is installed.</p> <p>It is also highly advisable that Administrators manually scan the permissions on various partitions on the system and ensures that they are appropriately secured for various user accesses in their environment.</p> <p>You see the recommended permission in the script.</p>		X	By Compass-Script
7006	Protect access to the boot partition	<p>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa</p> <p>Add/Change key value: Protect System Partition data type: REG_DWORD value: 1</p> <p>This is needed for architectures that require a non NTFS boot partition. Setting this key ensures that only Administrators may change data on this partition. Adding this value for other architectures has no side effects. Note that none of the architectures in the current evaluated configuration require the use of this key and therefore its effectiveness has not been assessed as part of the evaluation.</p>		X	to do by Hand



## 2.9 Logging and Monitoring

#	Logging and Monitoring	How to fix	L	N	Reference
8001*	Enabling System Auditing	<p>Enabling system auditing can inform you of actions that pose security risks and possibly detect security breaches.</p> <p>To activate security event logging, follow these steps:</p> <p>Click the Start button, point to Programs, point to Administrative Tools, and then click User Manager.</p> <ul style="list-style-type: none"> <li>• On the Policies menu, click Audit.</li> <li>• Click the Audit These Events option.</li> <li>• Enable the following options               <ul style="list-style-type: none"> <li>Audit account management Success: Failure</li> <li>Audit logon events Success: Failure</li> <li>Audit object access: Failure</li> <li>Audit policy change Success: Failure</li> <li>Audit privilege use: Failure</li> <li>Audit process tracking: No auditing</li> <li>Audit system events Success: Failure</li> </ul> </li> </ul> <p>Note: Files and folders must reside on an NTFS partition for security logging to be enabled. Once the auditing of file and object access has been enabled, use Windows NT Explorer to select auditing for individual files and folders.</p> <p>See Eventlog-Security for the messages generated by auditing. The Eventlog files are placed in /winnt/system32/config.</p>	X		By Compass-Script
8002*	Event log settings	<p>The Application, System and Security logs are configured to be up to 100MB each. They will overwrite events as needed, but only entries older than 30 days. The Event-</p>	X		to do by Compass-Script



#	Logging and Monitoring	How to fix	L	N	Reference
		<p>Logs stored in /winnt/system32/config/</p> <p>Administrative Tools (Common)-Event Viewer-Log-Log Settings</p>			
8003	Your machine will crash if it fails to Audit System / Application / Security Events	<p>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa</p> <p>Add/change a DWORD-Value named CrashOnAuditFail with a 1 in it.</p> <p><b>Note</b> knowledge base article Q140058 describes how to recover a machine that has crashed following audit trail exhaustion. In addition it should be noted that a Blue screen will now be generated when attempting to shut down a machine as explained in knowledge base article Q178208. Local procedures should be established to ensure that end-users do not attempt to reboot their machines when this event occurs.</p>	X		to do by Hand



## 2.10 General

#	General	How to fix	L	N	Reference
9001*	Update the system Emergency Repair Disk	You should update the system's Emergency Repair Disk (ERD) to reflect these changes. Remember to use the emergency repair disk, rather than the Restore utility, if system files are lost. Use the command <code>rdisk /s</code> . After creating ERD delete <code>/winnt/repair/sam._</code>	X		to do by hand
9002*	Subscribe to the Microsoft Security Notification Service	<b>Warning</b> You MUST keep on top of new security issues as they arise.  You can stay abreast of Microsoft-related security issues and fixes here ( <a href="http://www.microsoft.com/technet/security/notify.asp">http://www.microsoft.com/technet/security/notify.asp</a> ). You will receive notice of security issues by email. You should also consider placing a 'favorites shortcut' to the Microsoft Security Advisor Program.	X	X	to do by hand



### 3 Hardening Internet Information Server 4.0

#### 3.1 How to read the table

H = Hardening

L = Task influences local security aspects

N = Task influences network security aspects

No.	Description	How to fix	H		Reference
number	short brief description of the problem	discussion how to fix the problem	L	N	what script might automate this task

For hardening IIS it is necessary to fulfill the hardening task for the OS first. The following recommendations are based on a hardened OS. You have to decide by yourself which issues are required by your system and installation. It is possible that your application will stop, if you go trough the list without consideration about your configuration.



### 3.2 Installation

#	Installation	How to fix	L	N	Reference	
10001*	Change the default directories during the installation.	Do not use the default directories like \inetpub or \wwwroot. Take self created directory names like \webroot or \httpdoc.		X	to do by hand	
10002*	Create the Document-Root and Virtual Directories on a different Partition than the system.	During the creation of new virtual servers, configure the document root's on different partition than the system. If needed copy the default server files (c:\inetpub\wwwroot\ to another partition and reconfigure the default website using the internet service manager.		X	to do by hand	
10003	Install minimal Internet services required	It is generally considered good practice to reduce the number of entry points into a server, for Windows NT this means reducing the number of services. You should stop and disable unneeded services using the Service Configuration Manager. The following services must be running to use IIS (Depends about your Website!):		X	to do by hand	
		EventLog				Records events in the system, security, and application logs.
		NT LM Security Support Provider				Provides WinNT Security to remote procedure call programs that use transports other than named pipes.
		Remote Procedure Call (RPC) Locator				The Remote Procedure Call Locator service allows distributed applications to use the RPC Name service. The RPC Locator service manages the RPC Name service database.
		Remote Procedure Call (RPC) Service				The RPC subsystem includes the endpoint mapper and other miscellaneous RPC services.
		IIS Admin Service				Allows administration of Web and FTP



#	Installation	How to fix	L	N	Reference
		services through the Internet Information Services snap-in.			
		MSDTC			
		World Wide Web Publishing Service			
		Protected Storage			
		A service coming from the IE development team, starting with IE4. NT uses PS to encrypt and store secure info like SSL certificates, passwords for apps (like Outlook, Outlook Express, etc.), info stored by Profile Assistant, info maintained by MS Wallet, and digitally signed S/MIME keys.			
		The following Services may be required			
		Certificate Authority			
		Content Index			
		FTP Publishing Service			
		NNTP Service			
		Plug and Play			
		Remote Access Services			
		RPC Locator			
		Server Service			
		SMTP Service			
		Telephony Service			
		Uninterruptible Power Supply			
		Workstation			

### 3.3 Authentication, Encryption and protecting confidential data

#	Auth., Encryp. and Protect.	How to fix	L	H	Reference
11001	Set appropriate authentication methods	<p>These are application specific but you need to make sure you use 'strong enough' authentication for your application. The following lists the authentication schemes supported by IIS4 in increasing trust:</p> <ul style="list-style-type: none"> <li>• Anonymous</li> <li>• Basic</li> <li>• Windows NT Challenge/Response</li> <li>• Client Certificates</li> </ul> <p>Refer to [KBBase] Q229694 for further details. Consult also the following advisory <a href="http://www.nextgenss.com/advisories/iisauth.txt">http://www.nextgenss.com/advisories/iisauth.txt</a></p>		X	to do by hand
11002	Set up Secure Sockets Layer for passing usernames, passwords and confidential data.	SSL/TLS can be used to secure data as it's transferred from the client to the web server. SSL/TLS is used mainly when passwords or credit cards are to be transferred across the Internet. However, using SSL/TLS is slow, especially during the initial handshake, so keep pages that use SSL/TLS to a minimum and keep the content minimal.		X	to do by hand
11003*	Index Server only indexing documentation	Check what documents you are indexing, make sure you are not indexing confidential sources like sam._ or passwd.txt.		X	to do by hand



### 3.4 File- and Object Permissions/Logging

#	Permissions/Logging	How to fix	L	H	Reference										
12001	Set appropriate virtual directory permissions/Web application space	<p>This is also application dependant, but the following rules-of-thumb apply:</p> <table border="1"> <thead> <tr> <th>File Type</th> <th>ACL</th> </tr> </thead> <tbody> <tr> <td><b>CGI etc</b> .EXE, .DLL, .CMD, .PL</td> <td>Everyone (RX) Administrators (Full Control) System (Full Control)</td> </tr> <tr> <td><b>Script Files</b> .ASP etc</td> <td>Everyone (RX) Administrators (Full Control) System (Full Control)</td> </tr> <tr> <td><b>Include Files</b> .INC, .SHTML, .SHTM</td> <td>Everyone (RX) Administrators (Full Control) System (Full Control)</td> </tr> <tr> <td><b>Static Content</b> .HTML, .GIF, .JPEG</td> <td>Everyone (R) Administrators (Full Control) System (Full Control)</td> </tr> </tbody> </table> <p>Rather than setting ACLs on each file, you are better off setting new directories for each type of file and setting ACLs on the dir and allow the ACLs to inherit to the files. For example a directory structure may look like this:</p> <pre>c:\inetpub\wwwroot\myserver\static (.html) c:\inetpub\wwwroot\myserver\include (.inc) c:\inetpub\wwwroot\myserver\script (.asp) c:\inetpub\wwwroot\myserver\executable (.dll) c:\inetpub\wwwroot\myserver\images (.gif, .jpeg)</pre> <p>Also be aware that two directories need special attention:</p> <pre>c:\inetpub\ftproot (FTP server) c:\inetpub\mailroot (SMTP server)</pre>	File Type	ACL	<b>CGI etc</b> .EXE, .DLL, .CMD, .PL	Everyone (RX) Administrators (Full Control) System (Full Control)	<b>Script Files</b> .ASP etc	Everyone (RX) Administrators (Full Control) System (Full Control)	<b>Include Files</b> .INC, .SHTML, .SHTM	Everyone (RX) Administrators (Full Control) System (Full Control)	<b>Static Content</b> .HTML, .GIF, .JPEG	Everyone (R) Administrators (Full Control) System (Full Control)		X	to do by hand
File Type	ACL														
<b>CGI etc</b> .EXE, .DLL, .CMD, .PL	Everyone (RX) Administrators (Full Control) System (Full Control)														
<b>Script Files</b> .ASP etc	Everyone (RX) Administrators (Full Control) System (Full Control)														
<b>Include Files</b> .INC, .SHTML, .SHTM	Everyone (RX) Administrators (Full Control) System (Full Control)														
<b>Static Content</b> .HTML, .GIF, .JPEG	Everyone (R) Administrators (Full Control) System (Full Control)														



#	Permissions/Logging	How to fix	L	H	Reference
		They are both Everyone (Full Control) and should be overridden with something tighter depending on your level of functionality. Place the folder on a different volume to the IIS server if you are going to support Everyone (Write).			
12002*	Set appropriate IIS log file ACLs	<p>Make sure the ACLs on the IIS-generated log files (%systemroot%\system32\LogFiles) are:</p> <ul style="list-style-type: none"> <li>Administrators (Full Control)</li> <li>System (Full Control)</li> </ul> <p>This is to help prevent malicious users deleting the files to cover their tracks.</p>		X	to do by hand
12003*	Logging enabled	<p>Logging is paramount when you want to see if your server is being attacked. You should use W3C Extended Logging format by</p> <p>Loading the IIS MMC tool   Right-click on site in question   Properties   Web Site   Enable Logging (W3C Extended Log), then set the following properties:</p> <p>Date, Time, Client IP Address, User Name, Method, URI Stem, HTTP Status, User Agent, Server IP Address, Server Port, Referrer</p>		X	to do by hand
12004	Move the Logfiles from the systemdrive	Move the logfiles from the systemdrive to another partition using the Internet Service Manager (Highlight the virtual server – rightclick properties – Tab WebSite – Logging Properties – Log File Directory.		X	to do by hand
12005*	Secure the Internet Guest User account:	In User Manager: Under Local users and groups rename Internet Guest Account to an obscure name. Set a STRONG PASSWORD. Remove the renamed Internet Guest Account from the guest group.		X	to do by hand



#	Permissions/Logging	How to fix	L	H	Reference
		<p>Permissions: Set permissions for the renamed Internet Guest Account on all volumes to "No Access". Change the renamed Internet Guest Account permissions to "Read Only" for a few specific directories in order to allow the web server to function properly.</p> <p>Configure IIS to use the renamed user as guest account: MMC-Webserver-Properties-Directory Security-Authentication Methods-Account for Anonymous Access-Edit-Chose the renamed Account.</p>			

### 3.5 Removing unused stuff and features

#	Removing unused stuff	How to fix	L	H	Reference																
13001*	Disable or remove all sample applications	<p>Samples are just that, samples, they are not installed by default and should never be installed on a production server. This includes documentation (the SDK docs include sample code), the Exploration Air sample site and others. Here are the default</p> <table border="1"> <thead> <tr> <th>Technology</th> <th>Location</th> </tr> </thead> <tbody> <tr> <td>IIS</td> <td>c:\inetpub\iissamples</td> </tr> <tr> <td>IIS SDK</td> <td>c:\inetpub\iissamples\sdk</td> </tr> <tr> <td>Admin Scripts</td> <td>c:\inetpub\AdminScripts c:\inetpub\scripts</td> </tr> <tr> <td>Admin Samples</td> <td>c:\winnt\system32\inetsrv\adminsamples</td> </tr> <tr> <td>IISADMPWD</td> <td>c:\winnt\system32\inetsrv\iisadmpwd</td> </tr> <tr> <td>IISADMIN</td> <td>c:\winnt\system32\inetsrv\iisadmin</td> </tr> <tr> <td>Data access</td> <td>c:\Program Files\Common Files\System\msadc\Samples</td> </tr> </tbody> </table>	Technology	Location	IIS	c:\inetpub\iissamples	IIS SDK	c:\inetpub\iissamples\sdk	Admin Scripts	c:\inetpub\AdminScripts c:\inetpub\scripts	Admin Samples	c:\winnt\system32\inetsrv\adminsamples	IISADMPWD	c:\winnt\system32\inetsrv\iisadmpwd	IISADMIN	c:\winnt\system32\inetsrv\iisadmin	Data access	c:\Program Files\Common Files\System\msadc\Samples		X	to do by hand partly by IISLock Tool
Technology	Location																				
IIS	c:\inetpub\iissamples																				
IIS SDK	c:\inetpub\iissamples\sdk																				
Admin Scripts	c:\inetpub\AdminScripts c:\inetpub\scripts																				
Admin Samples	c:\winnt\system32\inetsrv\adminsamples																				
IISADMPWD	c:\winnt\system32\inetsrv\iisadmpwd																				
IISADMIN	c:\winnt\system32\inetsrv\iisadmin																				
Data access	c:\Program Files\Common Files\System\msadc\Samples																				



#	Removing unused stuff	How to fix	L	H	Reference
13002	Disable or remove unneeded COM Components	Some COM components are not required for most applications and should be removed. Most notably consider disabling the File System Object component, however, this will also remove the Dictionary object. Be aware that some programs may require components you are disabling. For example, Site Server 3.0 uses the File System Object. The following will disable the File System Object:  System Object: regsvr32 scrrun.dll /u		X	to do by hand
13003*	Remove some unused virtual directory	This directories should be removed if this feature is not required or if the server is on the Web. Refer to [KBase] Q184619 for more info about this functionality.  <ul style="list-style-type: none"> <li>• IISamples</li> <li>• Scripts</li> <li>• IISAdmin</li> <li>• IISHelp</li> <li>• IISADMPWD (This directory allows you to reset Windows NT passwords)</li> </ul>		X	to do by hand  partly by IISLock Tool
13004	Remove Unused Script Mappings	IIS is preconfigured to support common filename extensions such as .ASP and .SHTM. When IIS receives a request for a file of one of these types the call is handled by a DLL. If you don't use some of these extensions or functionality you should remove the mappings by open Internet Services Manager then right-clicking the Web server   Properties   Master Properties   WWW Service   Edit   HomeDirectory   Configuration and remove these references:		X	to do by hand  partly by IISLock Tool



#	Removing unused stuff	How to fix	L	H	Reference								
		<table border="1"> <tr> <td>If you don't use</td> <td>Remove this entry</td> </tr> <tr> <td>Web-based Password Reset</td> <td>Htr, hta</td> </tr> <tr> <td>Internet Database Connector</td> <td>idc</td> </tr> <tr> <td>Server-side includes</td> <td>.shtm, .stm, .shtml</td> </tr> </table>	If you don't use	Remove this entry	Web-based Password Reset	Htr, hta	Internet Database Connector	idc	Server-side includes	.shtm, .stm, .shtml			
If you don't use	Remove this entry												
Web-based Password Reset	Htr, hta												
Internet Database Connector	idc												
Server-side includes	.shtm, .stm, .shtml												
13005*	Disable RDS support	<p>This is an extremely important setting</p> <p>When incorrectly configured Remote Data Services can make a server vulnerable to denial of service and arbitrary code execution attacks. You should either remove the capability or restrict it's usage using ACLs. Refer to MS98-004, MS99-025 and [KBase ] Q184375 for more info. Also, check your IIS logs regularly for signs of attack, the signature to look for is something like:</p> <p>2001-5-24 20:38:12 - POST /msadc/msadcs.dll ...</p> <p>You can automate the searching process by using commend:</p> <pre>find /i "msadcs" logfile.log</pre>		X	to do by hand								
13005*	Check <FORM> input in your ASP code	<p>Many sites use input from a user to call other code or build SQL statements directly. In other words they are treating the input as valid, well formed, non-malicious input. This should not be so, there are a number of attacks, most notably on Unix where user input was treated incorrectly as valid input and the user gained access to the server or caused damage. You should always check all user &lt;FORM&gt; input before passing it onto another process or method call which may use an external resource such as the file system or a database.</p>		X	to do by hand								



#	Removing unused stuff	How to fix	L	H	Reference
13006	Disable Parent Paths	Parent Paths allows you to use '..' in calls to MapPath and the like. By default this option is enabled and should be disabled. To disable this option go to the root of the Web site , right click select Properties   Home Directory   Configuration   App Options and uncheck Enable Parent Path. Be sure that your apps not use parent paths.		X	to do by hand
13007*	Disable calling the command shell with #exec	The command can be used to call arbitrary commands at the Web server from within an HTML page. IIS disables this by default. You can double-check this by making sure the following is set to zero or is missing:  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\SSIEnableCmdDirective  This is a REG_DWORD Value and should be set to 0.		X	to do by hand
13008	Disable IP Address in Content-Location	The Content-Location header may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server. Refer to [KBase] Q218180 for further information about disabling this option.		X	to do by hand
13009	IP Address in the Basic Realm	If you telnet a IIS and try to get a password protected directory (HEAD /siteserver/admin HTTP/1.0) you will get the following information:  HTTP/1.1 401 Access Denied WWW-Authenticate: NTLM WWW-Authenticate: Basic realm="180.13.11.233"  There is no possibility to prevent this output. You should remove the Site Server HTTP Admin Interface and this Password protected Dir anyway. Also remove all unneeded protected directories.		X	to do by hand
13010	Set appropriate Frontpage Server Extensions ACL's	\Program Files\Common Files\Microsoft Shared\Web Server Extensions\ (and subdirectories)  Administrators (Full Control)		X	to do by hand



#	Removing unused stuff	How to fix	L	H	Reference
		SYSTEM (Full Control) Everyone (Read) \Program Files\Common Files\Microsoft Shared\Web Server Extensions\40\Admisapi (and subdirectories) Administrators (Full Control) SYSTEM (Read) Computername Admins (read)			
13011*	Remove Frontpage Server Extensions, when not needed.	Directories in the Webroot holds Dir's like _vti_ it itself. Uninstall it if not needed. You can do it in the Option Pack Setup		X	to do by hand

### 3.6 Miscellaneous

#	Miscellaneous	How to fix	L	H	Reference
14001	Disable the default website.	In Internet Service Manager: right-click on the "Default Web Site" and select [Stop]. Note: Do not use the default website and disable/delete the administrative one.		X	to do by hand
14002	Configure your own error messages	You will find it on MMC-Server-Properties-Master Properties-Edit-Custom Errors		X	to do by hand

### 3.7 Patches

#	Patches	How to fix	L	H	Reference
15001*	Update MDAC (Microsoft Data Access Components).	<p>During the IIS install, you installed MDAC, got version 1.5. This will still be 1.5 even if you applied service packs.</p> <p>There are several version in use. You can find a list at <a href="http://www.microsoft.com/data/mdac21info/manifest_intro.htm">http://www.microsoft.com/data/mdac21info/manifest_intro.htm</a></p> <p>The latest release 2.7 RTM, runs on XP, W2K and NT 4. You can find it at <a href="http://www.microsoft.com/data/download_270rtm.htm">http://www.microsoft.com/data/download_270rtm.htm</a></p> <p>Internet Explorer 4.0 SP2 is required! Install it with all patches.</p>		X	to do by hand
15002*	Apply the latest Security Patches for IIS	<p>Many Bug's coming up during the time concerning IIS. It's necessary to keep the fixes up to date. Check out Chapter 4.4 and <a href="http://www.microsoft.com/downloads/search.asp">http://www.microsoft.com/downloads/search.asp</a></p>		X	to do by hand



## 3.8 Tools from Microsoft

### 3.8.1 Lockdown Tool

IIS Lockdown Wizard version 2.1 works by turning off unnecessary features, thus reducing attack surface available to attackers. To provide multiple layers of protection against attackers, URLScan, with customized templates for each supported server role, is integrated into the IIS Lockdown Wizard. To keep the server completely secure, however, all hotfixes are required before and after applying IIS Lockdown Wizard to stay protected against known security vulnerabilities.

See <http://www.microsoft.com/technet/security/tools/locktool.asp>

### 3.8.2 URLScan

URLScan screens all incoming requests to an IIS web server, and only allows ones to pass that comply with a ruleset created by the administrator. This significantly improves the security of the server by helping ensure that it only responds to valid requests. The tool allows the administrator to filter requests based on length, character set, content and other factors. A default ruleset is provided, which can be customized to meet the needs of a particular server.

URLScan is working as an ISAPI-Filter. All Files (Binary, Log- and Configurationfile) will located in %SYSTEMROOT%\system32\inetrv\urlscan.

Lockdown Tool will install URLScan. You can also download it separately.

See <http://www.microsoft.com/technet/security/urlscan.asp>

The Internet Information Services (IIS) security tools, IISlockD and URLScan, must be configured appropriately for Exchange (OWA). See the article on the following URL:

<http://support.microsoft.com/support/kb/articles/Q309/5/08.asp>



## 4 Appendix

### 4.1 Tools

Note: Both SSH-Server need cmd.exe!!!

Tool	Description	URL
SSH	SSH Server for NT Servers	<a href="http://www.ssh.com/products/ssh">http://www.ssh.com/products/ssh</a>
VNC	A remote control Software like PCAnywhere – for free!	<a href="http://www.uk.research.att.com/vnc">http://www.uk.research.att.com/vnc</a>
OPENSSSH	SSH Server for NT Servers (Free Version with SFTP!)	<a href="http://www.networksimplicity.com/openssh">http://www.networksimplicity.com/openssh</a>

### 4.2 Resources

What	Description	URL
Microsoft Knowledge Base	Lot's of technical Papers and the famous KBASE-Articles, they are named like Q234628.	<a href="http://search.support.microsoft.com">http://search.support.microsoft.com</a>
Microsoft Security Pages	Lot's of information an downloads (i.e. Checklists)	<a href="http://www.microsoft.com/security">http://www.microsoft.com/security</a>



Microsoft Resource Kit	The Resource Kits help IT professionals deploy, manage, and support Windows NT. It comes with a lot of usefully tools. The Resource-Kit is included by Microsoft Technet CD Subscription.	<a href="http://www.microsoft.com/ntserver/nts/downloads/recommended/ntkit/default.asp">http://www.microsoft.com/ntserver/nts/downloads/recommended/ntkit/default.asp</a> <a href="http://www.microsoft.com/NTWorkstation/downloads/Recommended/Featured/NTKit.asp">http://www.microsoft.com/NTWorkstation/downloads/Recommended/Featured/NTKit.asp</a>
HideAway.net	Security Portal – with a lot of stuff.	<a href="http://www.hideaway.net/Server_Security/Library/Windows_2000_NT/windows_2000_nt.html">http://www.hideaway.net/Server_Security/Library/Windows_2000_NT/windows_2000_nt.html</a>

### 4.3 Utilities

Tool	Description	URL
DCOMCNFG	The DCOM Configuration tool can be used to configure 32-bit COM and DCOM applications. To run this tool, click Start, click Run, and then type dcomcnfg.	Included in Windows NT 4.0 WKS and SRV.
DISKMON	This utility captures all hard disk activity or acts like a software disk activity light in your system tray.	<a href="http://www.sysinternals.com/ntw2k/utilities.shtml">http://www.sysinternals.com/ntw2k/utilities.shtml</a>
DUMPSEC	DumpSec dumps the permissions (DACLS) and audit settings (SACLs) for the file system, registry, printers, shares user, group and replication information in a concise, readable listbox format, so that holes in system security are readily.	<a href="http://www.systemtools.com/somarsoft/">http://www.systemtools.com/somarsoft/</a>
FILEMON	This monitoring tool lets you see all file system activity.	<a href="http://www.sysinternals.com/ntw2k/utilities.shtml">http://www.sysinternals.com/ntw2k/utilities.shtml</a>
FPORT	Reports all open TCP/IP and UDP ports and maps them to the running application.	<a href="http://www.foundstone.com/rdlabs/tools.php">http://www.foundstone.com/rdlabs/tools.php</a>



	owning application.	
NTFSDOS	Access NTFS drives for read-only access from DOS.	<a href="http://www.sysinternals.com/ntw2k/utilities.shtml">http://www.sysinternals.com/ntw2k/utilities.shtml</a>
REGEDT32	The regedt32 can be used to configure the Registry. There is also an another tool called regedit available. Permission on Registry-Key can only set by using regedt32.	Included in Windows NT 4.0 WKS and SRV.
REGMON	This monitoring tool lets you see all Registry activity.	<a href="http://www.sysinternals.com/ntw2k/utilities.shtml">http://www.sysinternals.com/ntw2k/utilities.shtml</a>
TCPVIEW	See all open TCP and UDP endpoints.	<a href="http://www.sysinternals.com/ntw2k/utilities.shtml">http://www.sysinternals.com/ntw2k/utilities.shtml</a>

#### 4.4 Security Related Hotfixes after SP6a

(SP6a was release November 30, 1999)

See <http://www.microsoft.com/downloads/search.asp> (Product Name: IIS 4.0; OS: NT.4) for the latest Hotfixes.

The following patches are only NT Server and IIS related. Internet Explorer and other Server-Software (e.g. Exchange, SQL,...) need many other patches!

Date	Vulnerability	[KBase]
22 May 2002	Windows NT4.0 Security Patch: Local Privilege Elevation through Debugging Vulnerability	Q320206
23 Apr 2002	Windows NT 4.0 Server, Terminal Server Edition Security Rollup Package English	Q317636
10 Apr 2002	Windows NT 4.0 Security Patch: Internet Information Services Security Roll-up Package	Q319733
2 Apr 2002	Windows NT 4.0 Security Patch: Unchecked buffer in the Multiple UNC Provider	Q312895
7 Mar 2002	Windows 98 NT4 Security Patch: Unchecked Buffer in Windows Shell Could Lead to Code Execution	4.01_sp2



V0.96 – Hardening WindowsNT

5 Mar 2002	Windows NT4.0 Security Patch: Unchecked Buffer in Windows Shell Could Lead to Code Execution	Q313829
13 Feb 2002	Windows NT4.0 Security Patch: Memory Leak in SNMP Vulnerability	Q314147
3 Dec 2001	Windows NT4.0 Patch: Security Roll-Up Fix Q299444 May Cause Lexmark Printers to Stop Responding	Q310703
6 Sep 2001	Windows NT4.0 Security Patch: Malformed Request to RPC Endpoint Mapper can Cause RPC Service to Fail	Q305399
22 Aug 2001	Windows NT4.0 Security Patch: Hyperterminal Buffer Overflow Vulnerability	Q304158
21 Aug 2001	Windows NT4.0 Security Patch: Invalid Digital Signature Error Occurs after installing NT4.0 SRP	Q305929
13 Aug 2001	Windows NT4 Security Patch: Multiple NNTP Posts can consume Memory	Q304876
23 Jul 2001	Windows NT4.0 Security Patch: Memory Leak in Telnet Server	Q301514
23 Jul 2001	Windows NT4.0 Security Patch: Denial-of-Service Attack with SFU 2.0	Q294380
23 Jul 2001	<p>Post-Windows NT 4.0 Service Pack 6a Security Rollup Package (SRP). The patches above are not included in the this package. You have to install these patches separately.            For further information look here <a href="http://support.microsoft.com/support/kb/articles/q299/4/44.asp?ID=299444">http://support.microsoft.com/support/kb/articles/q299/4/44.asp?ID=299444</a></p> <p><b>If you have installed the Compaq Array Controller Driver (Cpqarray.sys) see Q305228. Your Computer may have a bluescreen after installing SRP!</b></p>	Q299444



## 4.5 How to find Security Fixes

### 4.5.1 Microsoft Network Security Hotfix Checker (HFNetChk)

You can use the Hfnetchk tool to assess patch status for computers that are running Windows NT 4.0, Windows 2000, and Windows XP, as well as hotfixes for Internet Information Server 4.0 (IIS), Internet Information Services 5.0 (IIS), SQL Server 7.0, SQL Server 2000 (including Microsoft Data Engine [MSDE]), and Internet Explorer 5.01 or later.

See <http://support.microsoft.com/support/kb/articles/q3032/15.asp>

Note: This Tool may stop work on hardened systems!

### 4.5.2 Microsoft Download Center

Go to <http://www.microsoft.com/downloads/searchdl.asp>

Chose “Keyword Search” and type security in

Chose your Operating System e.g. Windows NT 4.0

## 4.6 Portlist

Windows NT		Convoy Clustering (WLBS)	
Browsing	UDP:137,138	Convoy	UDP:1717
DHCP Lease	UDP:67,68	WLBS	UDP:2504
DHCP Manager	TCP:135	<b>Exchange</b>	
Directory Replication	UDP:138 TCP:139	Client/Server Comm.	TCP:135
DNS Administration	TCP:135	Exchange Administrator	TCP:135
DNS Resolution	UDP:53	IMAP	TCP:143



Event Viewer	TCP:139	IMAP (SSL)	TCP:993
File Sharing	TCP:139	LDAP	TCP:389
Logon Sequence	UDP:137,138 TCP:139	LDAP (SSL)	TCP:636
NetLogon	UDP:138	MTA - X.400 over TCP/IP	TCP:102
Pass Through Validation	UDP:137,138 TCP:139	POP3	TCP:110
Performance Monitor	TCP:139	POP3 (SSL)	TCP:995
PPTP	TCP:1723 IP Protocol:47 (GRE)	RPC	TCP:135
Printing	UDP:137,138 TCP:139	SMTP	TCP:25
Registry Editor	TCP:139	NNTP	TCP:119
Server Manager	TCP:139	NNTP (SSL)	TCP:563
Trusts	UDP:137,138 TCP:139	<b>Terminal Server</b>	
User Manager	TCP:139	RDP Client (Microsoft)	TCP:3389 (Pre Beta2:1503)
WinNT Diagnostics	TCP:139	ICA Client (Citrix)	TCP:1494
WinNT Secure Channel	UDP:137,138 TCP:139		
WINS Replication	TCP:42		
WINS Manager	TCP:135		
WINS Registration	TCP:137		

#### 4.7 Compass Script

The Script and Registry-File processes the changes which are marked as “to do by Compass-Script” in the tables above. The tools used in the script are included in the Microsoft Resource Kit for NT Server. Please feel free to edit these files to fit in your needs. You can download the scripts and the necessary tools here <http://www.csnc.ch/downloads/docs/hardening/hardennt.zip>. A few of unused Registry-Params are already included in the hardennt.reg.