



Hardening WindowsNT

Compass Security

Draft V0.81

April 6th, 2001

Document name:	Hardening_WindowsNT_CSNC_V0.81.pdf
Version:	Draft V0.81
Author:	Christoph Schnidrig, Compass Security AG christoph.schnidrig@csnc.ch http://www.csnc.ch
References:	a couple of other hardening doc / experience
Date of delivery:	April 6, 2001
Document state:	PUBLIC



CONTENT

1	INTRODUCTION.....	1
	1.1 <i>Version control</i>	1
	1.2 <i>Local - Network - Application Security</i>	2
2	HARDENING WINDOWS NT 4.0.....	4
	2.1 <i>How to read the table</i>	4
	2.2 <i>Installation</i>	5
	2.3 <i>System</i>	6
	2.4 <i>User Management</i>	10
	2.5 <i>Services included by WindowsNT</i>	14
	2.6 <i>Secure Network Settings</i>	17
	2.7 <i>Administering</i>	21
	2.8 <i>File/Registry Permissions</i>	23
	2.9 <i>Logging and Monitoring</i>	25
	2.10 <i>General</i>	27
3	APPENDIX.....	28
	3.1 <i>Tools</i>	28
	3.2 <i>Resources</i>	28
	3.3 <i>Utilities</i>	29
	3.4 <i>Portlist</i>	30
	3.5 <i>Compass script</i>	31



1 Introduction

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

- Network security
- Local security

aspect.

This document is still a draft and Compass is working on it.

1.1 Version control

Version	Author	Description	Filename
0.80	Christoph Schnidrig christoph.schnidrig@csnc.ch	Initial version saved on http://www.csnc.ch/download	Hardening_WindowsNT_CSNC_V0.80.pdf
0.81	Christoph Schnidrig	Some minor changes, Add some notes.	Hardening_WindowsNT_CSNC_V0.81.pdf

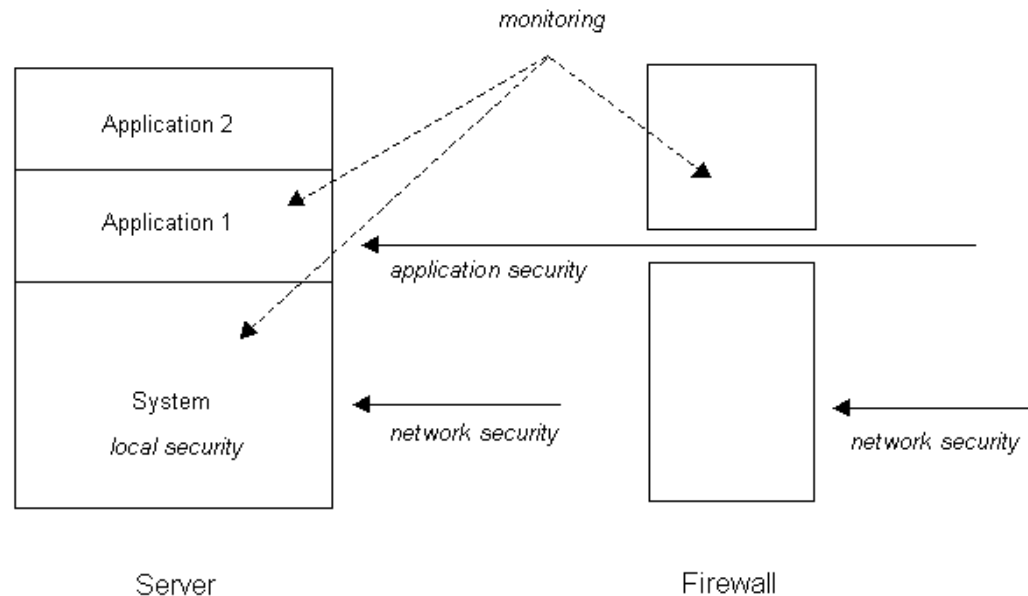
[Christoph] I would like to improve the checklist as well. But as you know---time is the problem. If you feel like having something you would like to see in this document, pls. let me know. I will leave the version control chapter in the future. So everybody can see who did what on this document.

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, IIS Security 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 and the Microsoft Checklists are available at 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-Step this Scripts is called Compass-Script. This script include 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 or not. You have the Background what application and function have to run on your machine.

2.2 Installation

#	Installation	How to fox	L	N	Reference
1001	Install available hotfixes	<p>Install all available hotfixes. The hotfixes are available from ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40</p> <p>To Check Versions of Installed Hotfixes see KBase Q238552, check HKLM\Software\Microsoft\Windows NT\CurrentVersion\Hotfix or run <code>winver</code>.</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, Word... from Server. If you really need a browser on the server, use Netscape instead Internet Explorer. There are many Exploids for IE (Active X-Stuff).	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\Services\Cdrom\Autorun Set its value to 0 to disable auto-run. (See KBase Q155217 and Q126309.)	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.	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.	X		to do by Compass-Script
2004	Disabling the Registry Editors	If the Registry key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System 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
2005	Shutting Down the System without logon	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	X		to do by Compass-Script

#	System	How to fix	L	N	Reference
		<p>“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!</p>			
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</p> <p>Delete OS2 and Posix key values</p> <p>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	Other potential dangerous tools	<p>arp.exe, at.exe, atsvc.exe, cacls.exe, cmd.exe, command.com, 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
2008	Wiping the System Page File during clean system shutdown	<p>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:</p>	X		to do by Compass-Script

#	System	How to fix	L	N	Reference
		setting up the following key: HKEY_LOCAL_MACHINE\SYSTEM\System\CurrentControlSet\Control\SessionManager\Memory Management\ClearPageFileAtShutdown (=1 REG_DWORD)			
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. 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.	X		to do by Hand
2011	System boot time set to zero seconds	Go to Control Panel-System-Startup/Shutdown and set „Show list for“ to zero.	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 Accessories-Clipboard Viewer and uncheck the box	X		to do by Hand

#	System	How to fix	L	N	Reference
		NT Setup-Accessoires-Clipboard Viewer and uncheck the box.			
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	<p>To enable stronger protection on base objects, add the following value to the registry key</p> <p>HKLM\SYSTEM\CurrentControlSet\Control\Session Manager</p> <p>Add/change a REG_DWORD-Value named ProtectionMode with a 1 in it.</p> <p>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 http://www.microsoft.com/technet/security/bulletin/ms99-006.asp</p>	X		

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: 10 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 to rename the guest account to administrator and enable the logging for failed logons. In this case you can see if a hacker tries to logon as administrator ;-) 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>Do not assign to any user.</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>Do not assign to any user.</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	Do not assign to any user.	Add workstations to domain	Domain Admins	Back up files and directories	trusted users (e.g. the Backup Operators group)	Bypass traverse checking	Authenticated Users	Change the system time	trusted users (e.g. Server Operators)	Create a pagefile	trusted users (e.g. Server Operators)	Create a token object	Do not assign to any user.	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	Do not assign to any user.																								
Add workstations to domain	Domain Admins																								
Back up files and directories	trusted users (e.g. the Backup Operators group)																								
Bypass traverse checking	Authenticated Users																								
Change the system time	trusted users (e.g. Server Operators)																								
Create a pagefile	trusted users (e.g. Server Operators)																								
Create a token object	Do not assign to any user.																								
Create permanent shared objects	(no one)																								

#	User Management	How to fix	L	N	Reference
		Debug programs (no one) This right is not auditable! Force shutdown from a remote sys. trusted users (e.g. Server Operators) Generate security audits Do not assign to any user. Increase quotas trusted users (e.g. Server Operators) Increase scheduling priority trusted users (e.g. Server Operators) Load and unload device drivers trusted users (e.g. Server Operators) Lock pages in memory (no one) Log on as a batch job trusted users (as needed) Log on as a service trusted users (as needed) Log on locally Trusted users (as needed) Manage auditing and security log trusted users (e.g. Domain Admins) Modify firmware environment value trusted users (e.g. Domain Admins) Profile single process trusted users Profile system performance trusted users Replace a process level token Do not assign to any user. Restore files and directories trusted users (e.g. Backup Operators) Shut down the system trusted users (e.g. Server Operators) Take ownership of files or 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 (http://www.l0pht.com/). 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
		Go to Display > Screen Saver > Logon Screen Saver and select Enable Password Protect. Click OK.			
3010	Enable network lockout of admin account.	Use the NT Resource Kit's passprop utility to run the following command: <pre>passprop /adminlockout /complex</pre> <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	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	X		to do by Compass-Script
3012	Restrict the ability to add printer drivers	“AddPrinterDrivers” with a REG_DWORD value of 1 in the Registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers Untrusted print drivers can maliciously divert user data.	X		to do by Compass-Script
3013	Prevent user from running Task Manager	HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\System\ Add/Change a REG_DWORD-Value named DisableTaskMgr with a 1 in it.	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 the following services</p> <p>Note: You have to check which service is needed by your application or not!</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				
	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 at 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 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.			

#	Services included by NT	How to fix	L	H	Reference								
		<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></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>	EventLog	Records events in the system, security, and application logs.	NT LM Security Support Provider		Remote Procedure Call (RPC) Service	The RPC subsystem includes the endpoint mapper and other miscellaneous RPC services.					
EventLog	Records events in the system, security, and application logs.												
NT LM Security Support Provider													
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	<p>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] Note: Set a strong password Click [OK] to accept changes. Click [OK] to close the MS SNMP Properties</p>		X	to do by Hand								
4003	Change the Scheduler service's security context	<p>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:</p> <ul style="list-style-type: none"> • Open the Services control panel (Start Settings Control Panel Services). • Select the Schedule service, then click the Startup button. The Service information dialog will appear. • 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. • Stop and restart the service. 		X	to do by Hand								

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	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\WINREG 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.		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: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa		X	to do by Compass-Script
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	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		X	to do by Hand

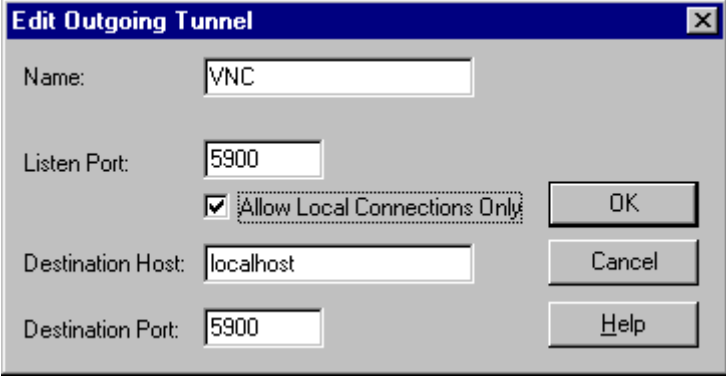
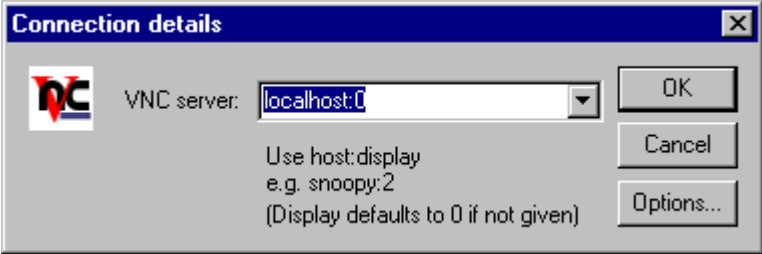
#	Network	How to fix	L	N	Reference
		Dynamic Data Exchange), and remote administration.			
5006	Configure TCP/IP filters Skip this step if you are to install another packet filtering software on this host later on.	Configure TCP/IP-security by specifying the ports that are allowed inbound (TCP or UDP) 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 http://www.isi.edu/in-notes/iana/assignments/port-numbers		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 named “EnablePlainTextPassword” with a REG_DWORD value of 1 to the Registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RDR\Parameters 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.		X	
5009	Configure Server Message Block authentication protocol	Require SMB signing of server and/or client activities by creating REG_DWORD values named “EnableSecuritySignature” and “RequireSecuritySignature” with a		X	to do by Hand

#	Network	How to fix	L	N	Reference
	Block authentication protocol	<p>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>			
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 requestet 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
5011	DCOM RPC high ports	<p>By default DCOM dynamically allocates one high port (>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 2reserved 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</p>		X	to do by Hand

#	Network	How to fix	L	N	Reference
		<p>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>			
5012	Set NTLM security to response only	<p>\HKLM\SYSTEM\CurrentControlSet\Control\LSA Add/change key value: LMCompatibilityLevel data type: REG_DWORD value: 2</p> <p>\HKLM\SYSTEM\CurrentControlSet\Control\LSA\MSV1_0 Add/change key value: NtLmMinClientSec data type: REG_DWORD value: 0</p> <p>Add/change key value: NtLmMinServerSec data type: REG_DWORD value: 0</p> <p>See KBase Q147706.</p>		X	

2.7 Administering

#	Administering	How to fix	L	H	Reference	
6001	<p>Setting up secure Administrating with SSH and VNC</p> <p>Note: 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>Used Software: SSH-Server (30Day Testversion): ftp://ftp.ssh.com/pub/ssh/SSHWinServer.exe SSH Client (non-commercial): ftp://ftp.ssh.com/pub/ssh/SSHWin-2.4.0-pl2.exe VNC: http://www.uk.research.att.com/vnc/dist/vnc-3.3.3r9_x86_win32.zip</p> <p>Installation Steps on the server machine: Install and start the VNC-Server. For more information about VNC have a look at: http://www.uk.research.att.com/vnc/</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>Installation Steps on the client machine:</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 Klick add</p>			X	to do by Hand

#	Administering	How to fix	L	H	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	H	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: Timeout data type: REG_DWORD</p>	X		to do by Hand

#	File/Registry Permissions	How to fix	L	H	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	H	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"> • On the Policies menu, click Audit. • Click the Audit These Events option. • Enable the following options <ul style="list-style-type: none"> Audit account management Success: 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 <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	H	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>Note 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	H	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	Warning You MUST keep on top of new security issues as they arise. You can stay abreast of Microsoft-related security issues and fixes here (http://www.microsoft.com/technet/security/notify.asp). 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 Appendix

3.1 Tools

Tool	Description	URL
SSH	SSH Server for NT Servers	http://www.ssh.com/products/ssh
VNC	A remote control Software like PCAnywhere – for free!	http://www.uk.research.att.com/vnc

3.2 Resources

What	Description	URL
Microsoft Knowledge Base	Lot's of technical Papers and the famous KBASE-Articles, they are named like Q234628.	http://search.support.microsoft.com
Microsoft Security Pages	Lot's of information an downloads (i.e. Checklists)	http://www.microsoft.com/security
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.	http://www.microsoft.com/ntserver/nts/downloads/recommended/ntkit/default.asp http://www.microsoft.com/NTWorkstation/downloads/Recommended/Featured/NTKit.asp
HideAway.net	Security Portal – with a lot of stuff.	http://www.hideaway.net/Server_Security/Library/Windows_2000_NT/windows_2000_nt.html

3.3 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.	http://www.sysinternals.com/ntw2k/utilities.shtml
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.	http://www.systemtools.com/somarsoft/
FILEMON	This monitoring tool lets you see all file system activity.	http://www.sysinternals.com/ntw2k/utilities.shtml
FPORT	Reports all open TCP/IP and UDP ports and maps them to the owning application.	http://www.foundstone.com/rdlabs/tools.php
NTFSDOS	Access NTFS drives for read-only access from DOS.	http://www.sysinternals.com/ntw2k/utilities.shtml
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.	http://www.sysinternals.com/ntw2k/utilities.shtml
TCPVIEW	See all open TCP and UDP endpoints.	http://www.sysinternals.com/ntw2k/utilities.shtml

3.4 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	Exchange	
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	Terminal Server	
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		

3.5 Compass script

The following 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 the files to fit in your needs. You can download the scripts and the necessary tools here <http://www.csnc.ch/downloads/sources/hardennt.zip> . A few of unused Registry-Params are already included in the hardennt.reg.

```
#####
# hardennt.cmd #
# written by Christoph Schnidrig #
# Compass Security 29.3.2001 #
#####

echo ----- >> hardennt.log
echo Run the regfile >> hardennt.log
echo ----- >> hardennt.log

regedit /s hardennt.reg >> hardennt.log

echo ----- >> hardennt.log
echo Remove OS2- and Posix Registry Values and Files >>
hardennt.log
echo ----- >> hardennt.log

rd /s /q %SYSTEMROOT%\system32\os2 >> hardennt.log

del /q /f %SYSTEMROOT%\system32\os2.exe >> hardennt.log
del /q /f %SYSTEMROOT%\system32\os2ss.exe >> hardennt.log
del /q /f %SYSTEMROOT%\system32\os2srv.exe >> hardennt.log
del /q /f %SYSTEMROOT%\system32\posix.exe >> hardennt.log
del /q /f %SYSTEMROOT%\system32\psxss.exe >> hardennt.log
del /q /f %SYSTEMROOT%\system32\psxdll.dll >> hardennt.log

reg delete HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\Environment\Os2LibPath /force >> hardennt.log
reg delete HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\SubSystems\Os2 /force >> hardennt.log
reg delete HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\SubSystems\Posix /force >> hardennt.log

echo ----- >> hardennt.log
```

```
echo Remove Critical Files from System32 to another ACL Directory
>> hardennt.log
echo ----- >> hardennt.log

md %SYSTEMDRIVE%\admintools >> hardennt.log
move %SYSTEMROOT%\system32\arp.exe %SYSTEMDRIVE%\admintools\arp.exe
>> hardennt.log
move %SYSTEMROOT%\system32\at.exe %SYSTEMDRIVE%\admintools\at.exe
>> hardennt.log
move %SYSTEMROOT%\system32\atsvc.exe
%SYSTEMDRIVE%\admintools\atsvc.exe >> hardennt.log
move %SYSTEMROOT%\system32\calcs.exe
%SYSTEMDRIVE%\admintools\calcs.exe >> hardennt.log
move %SYSTEMROOT%\system32\cmd.exe %SYSTEMDRIVE%\admintools\cmd.exe
>> hardennt.log
move %SYSTEMROOT%\system32\command.com
%SYSTEMDRIVE%\admintools\command.com >> hardennt.log
move %SYSTEMROOT%\system32\cscript.exe
%SYSTEMDRIVE%\admintools\cscript.exe >> hardennt.log
move %SYSTEMROOT%\system32\debug.exe
%SYSTEMDRIVE%\admintools\debug.exe >> hardennt.log
move %SYSTEMROOT%\system32\edit.com
%SYSTEMDRIVE%\admintools\edit.exe >> hardennt.log
move %SYSTEMROOT%\system32\edlin.exe
%SYSTEMDRIVE%\admintools\edlin.exe >> hardennt.log
move %SYSTEMROOT%\system32\finger.exe
%SYSTEMDRIVE%\admintools\finger.exe >> hardennt.log
move %SYSTEMROOT%\system32\ftp.exe %SYSTEMDRIVE%\admintools\ftp.exe
>> hardennt.log
move %SYSTEMROOT%\system32\ipconfig.exe
%SYSTEMDRIVE%\admintools\ipconfig.exe >> hardennt.log
move %SYSTEMROOT%\system32\nbtstat.exe
%SYSTEMDRIVE%\admintools\nbtstat.exe >> hardennt.log
move %SYSTEMROOT%\system32\net.exe %SYSTEMDRIVE%\admintools\net.exe
>> hardennt.log
```



```
move %SYSTEMROOT%\system32\netstat.exe
%SYSTEMDRIVE%\admintools\netstat.exe >> hardennt.log
move %SYSTEMROOT%\system32\nslookup.exe
%SYSTEMDRIVE%\admintools\nslookup.exe >> hardennt.log
move %SYSTEMROOT%\system32\ping.exe
%SYSTEMDRIVE%\admintools\ping.exe >> hardennt.log
move %SYSTEMROOT%\system32\qbasic.exe
%SYSTEMDRIVE%\admintools\qbasic.exe >> hardennt.log
move %SYSTEMROOT%\system32\rcp.exe %SYSTEMDRIVE%\admintools\rcp.exe
>> hardennt.log
move %SYSTEMROOT%\system32\rdisk.exe
%SYSTEMDRIVE%\admintools\rdisk.exe >> hardennt.log
move %SYSTEMROOT%\system32\regedit.exe
%SYSTEMDRIVE%\admintools\regedit.exe >> hardennt.log
move %SYSTEMROOT%\system32\regedt32.exe
%SYSTEMDRIVE%\admintools\regedt32.exe >> hardennt.log
move %SYSTEMROOT%\system32\rexec.exe
%SYSTEMDRIVE%\admintools\rexec.exe >> hardennt.log
move %SYSTEMROOT%\system32\route.exe
%SYSTEMDRIVE%\admintools\route.exe >> hardennt.log
move %SYSTEMROOT%\system32\rdisk.exe
%SYSTEMDRIVE%\admintools\rdisk.exe >> hardennt.log
move %SYSTEMROOT%\system32\rsh.exe %SYSTEMDRIVE%\admintools\rsh.exe
>> hardennt.log
move %SYSTEMROOT%\system32\runonce.exe
%SYSTEMDRIVE%\admintools\runonce.exe >> hardennt.log
move %SYSTEMROOT%\system32\secfixup.exe
%SYSTEMDRIVE%\admintools\secfixup.exe >> hardennt.log
move %SYSTEMROOT%\system32\syskey.exe
%SYSTEMDRIVE%\admintools\syskey.exe >> hardennt.log
move %SYSTEMROOT%\system32\telnet.exe
%SYSTEMDRIVE%\admintools\telnet.exe >> hardennt.log
move %SYSTEMROOT%\system32\tftp.exe
%SYSTEMDRIVE%\admintools\tftp.exe >> hardennt.log
move %SYSTEMROOT%\system32\tracert.exe
%SYSTEMDRIVE%\admintools\tracert.exe >> hardennt.log
move %SYSTEMROOT%\system32\wscript.exe
%SYSTEMDRIVE%\admintools\wscript.exe >> hardennt.log
move %SYSTEMROOT%\system32\xcopy.exe
%SYSTEMDRIVE%\admintools\xcopy.exe >> hardennt.log

echo ----- >> hardennt.log
echo ACL Critical Files and Directories >> hardennt.log
```

```
echo ----- >> hardennt.log
echo xcalcs directories >> hardennt.log
xcaccls %SystemRoot% /T /C /G Administrators:F SYSTEM:F "CREATOR
OWNER":F EVERYONE:R /Y >> hardennt.log
xcaccls %SystemRoot%\repair /T /C /G Administrators:F /Y >>
hardennt.log
xcaccls %SystemRoot%\config /T /C /G Administrators:F SYSTEM:F
"CREATOR OWNER":F EVERYONE:R /Y >> hardennt.log
xcaccls %SystemRoot%\system32\spool /T /C /G Administrators:F
SYSTEM:F "CREATOR OWNER":F "POWER USERS":C EVERYONE:R /Y >>
hardennt.log
xcaccls %SystemRoot%\cookies /T /C /G Administrators:F /Y >>
hardennt.log
xcaccls %SystemRoot%\forms /T /C /G "CREATOR OWNER":F /Y >>
hardennt.log
xcaccls %SYSTEMDRIVE%\admintools /T /C /G Administrators:F /Y >>
hardennt.log

echo xcalcs files >> hardennt.log
xcaccls c:\boot.ini /T /C /G Administrators:F SYSTEM:F /Y >>
hardennt.log
xcaccls c:\ntdetect.com /T /C /G Administrators:F SYSTEM:F /Y >>
hardennt.log
xcaccls c:\ntldr /T /C /G Administrators:F SYSTEM:F /Y >>
hardennt.log
xcaccls c:\autoexec.bat /T /C /G Administrators:F SYSTEM:F /Y >>
hardennt.log
xcaccls c:\autoexec.bat /T /C /G Administrators:F SYSTEM:F
EVERYONE:R /Y >> hardennt.log
xcaccls c:\autoexec.bat /T /C /G Administrators:F SYSTEM:F
EVERYONE:R /Y >> hardennt.log
xcaccls c:\config.sys /T /C /G Administrators:F SYSTEM:F EVERYONE:R
/Y >> hardennt.log

echo ----- >> hardennt.log
echo Prevent Windows NT from passing unencrypted passwords across
the network >> hardennt.log
echo by echoing the EnablePlainTextPassword value. >>
hardennt.log
echo ----- >> hardennt.log

reg delete
HKLM\SYSTEM\CurrentControlSet\Services\RDR\Parameters\EnablePlainTe
xtPassword /force >> hardennt.log
```



```
echo ----- >> hardennt.log
echo Enable the Systemlogging >> hardennt.log
echo ----- >> hardennt.log

auditpol /enable /system:Failure >> hardennt.log
auditpol /enable /logon:Failure >> hardennt.log
auditpol /enable /object:Failure >> hardennt.log
auditpol /enable /privilege:Failure >> hardennt.log
auditpol /enable /process:None >> hardennt.log
auditpol /enable /policy:Failure >> hardennt.log
auditpol /enable /sam:Failure >> hardennt.log

echo #####
echo # hardennt.cmd #
echo # written by Christoph Schnidrig #
echo # Compass Security 29.3.2001 #
echo #####
echo # is passed, please reboot the system. #
echo # See hardennt.log for details. #
echo #####
pause

REGEDIT4

#####
# hardennt.reg #
# written by Christoph Schnidrig #
# Compass Security 29.3.2001 #
#####

# -----
# regedit /s <registry file>.reg
# -----

# -----
# #2001 Disable CDROM Auto-Run
# -----

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom]
"Autorun"=dword:00000000

# -----
```

```
# #2002, #2003 Only the interactive user can access CDROM's and Floppies
# -----

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon]
"AllocateFloppies"="1"
"AllocateCdRoms"="1"

# -----
# #2005 Disable Shutting down the System without Logon
# -----

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon]
"ShutdownWithoutLogon"="0"

# -----
# #2006 Remove OS2 Subsystem
# -----

-[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT]
-[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT\1.0]
-[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for
NT\1.0\config.sys]
-[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for
NT\1.0\os2.ini]

# -----
# #2008 Wiping the System Page File during system shutdown
# -----

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\Memory Management]
"ClearPageFileAtShutdown"=dword:00000001

# -----
# #3002 Hiding the Last Username
# -----

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon]
"DontDisplayLastUserName"="1"

# -----
# #3009 Enable Screensaver with Passwordprotection
# -----
```



```
[HKEY_CURRENT_USER\Control Panel\Desktop]
"ScreenSaveTimeOut"="240"
"ScreenSaveActive"="1"
"ScreenSaverIsSecure"="1"
"SCRNSAVE.EXE"="C:\WINNT\black16.scr"

# -----
# #3011Disable Unauthenticated Event Log Viewing
# -----

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Appl
ication]
"RestrictGuestAccess"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Syst
em]
"RestrictGuestAccess"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Secu
rity]
"RestrictGuestAccess"=dword:00000001

# -----
# #3012 Restrict the installation of printer drivers to Admins and
Print Operators
# -----

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Provider
s\LanMan Print Services\servers]
"AddPrintDrivers"=dword:00000001

# -----
# #3013 Prevent user from running Task Manager
# -----

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Polic
ies\System]
"DisableTaskMgr"=dword:00000001

# -----
# #5003 Restrict anonymous connections to IPC$
# -----

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA]
```

```
"RestrictAnonymous"=dword:00000001

# -----
# #5004 Restrict Null Session Access over Named Pipes
# -----
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\
Parameters]
"NullSessionPipes"=""
"NullSessionShares"=""

# -----
# #5007 Disables administrative shares on a NT4.0 Server (eg: $c,
$d, $e etc)
# -----
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\
Parameters]
"AutoShareServer"=dword:00000000

# -----
# #5007 Disables administrative shares on a NT4.0 Workstation (eg:
$c, $d, $e etc)
# -----
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\
Parameters]
"AutoShareWks"=dword:00000000

# -----
# #5010 Prevent using LANMAN Password (Note: Windows95 and older
system stop able to connect!)
# -----
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\control\LSA]
"LMCompatibilityLevel"=dword:00000000

# -----
# #8002 Setting the Eventlog - Size 8000KB, Retention-Time 30 days
# -----

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Appl
ication]
"MaxSize"=dword:007d0000
"Retention"=dword:00278d00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Secu
rity]
"MaxSize"=dword:007d0000
"Retention"=dword:00278d00
```



```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System]
"MaxSize"=dword:007d0000
"Retention"=dword:00278d00
# -----
#####
# Additional Stuff
#####

# Secure base objects
#[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager]
#"ProtectionMode"=dword:00000001

#Displaying a Legal Notice Before Log On
#[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon]
#"LegalNoticeCaption"="This is the Caption"
#"LegalNoticeText"="This is is the legal Text"

# Your machine will crash if it fails to Audit System / Application
/ Security Events
#[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
#"CrashOnAuditFail"=dword:00000001

# Disable caching of logon information
#[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon]
#"CachedLogonsCount"="0"
#[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Param
eters]
#"DisableSavePassword"=dword:00000001

# Turn off NTFS 8.3 Name Generation
#[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem]
#"NtfsDisable8dot3NameCreation"=dword:00000001

#Enable RAS logging
#[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Param
eters]
#"Logging"=dword:00000001

#NT LSA DoS (Phantom) Vulnerability
```

```
#[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AeDebug]
#"Auto"="0"

#set MDAC to operate in safe [1] / unsafe [0] mode
#[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataFactory\HandlerInfo]
#"HandlerRequired"=dword:00000001

#Disable Lan Manager authentication, 0 - Send both WinNT and Lan
Manager passwd ; forms. 1 - Send Windows NT and Lan Manager
password forms if server requests it. 2 ; - Only send Windows NT
password form
#[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA]
#"LMCompatibilityLevel"=dword:00000002

#To disable DCOM, utilize the "DCOMCNFG.EXE" program, select
default properties and make sure ; that 'enable distributed COM on
this computer' box is deselected OR Set ; the following ; registry
key to disable the DCOM service:
#;[HKEY_LOCAL_MACHINE\Software\Microsoft\Ole]
#"EnabledCOM"="N"

#Enable TCP/IP Filtering
#[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parame
ters]
#"EnableSecurityFilters"=dword:00000001

#Disable ICMP Redirect
#[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parame
ters]
#"EnableICMPRedirect"=dword:00000000

#Disable' IP source routing
#[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parame
ters]
#"DisableIPSourceRouting"=dword:00000001

#Disallow Fragmented IP
#[HKEY_LOCAL_MACHINE\System\CurrentControlSet\IPFilterDriver\Parame
ters]
#"EnableFragmentChecking"=dword:00000001

#Disable forwarding of fragmented IP packets
#[HKEY_LOCAL_MACHINE\System\CurrentControlSet\IPFilterDriver\Parame
ters]
#"DefaultForwardFragments"=dword:00000000
```



```
#Disable IP Forwarding
#[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]
#"IPEnableRouter"=dword:00000000

#Fix for MS DNS Compatibility with BIND versions earlier than 4.9.4
#[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters]
#"BindSecondaries"=dword:00000001
```