Global Information Assurance Certification Paper

IT Services security plan

Hardening and Managing IIS 4 servers for the Internet.

Out of the box NT is seriously vulnerable to attack on the Internet, even behind a firewall. It needs to be hardened and managed as part of due diligence in securing information, systems, and services of value to all the stakeholders in the organization.

To aid in efficiency and IT quality control, and to complete the practical assignment for the SANS Institute NT Security certification, I have developed this plan and documentation, which will explain the proposed method of auditing NT security.

The plan includes:

- Establishing baseline requirements
- Methods of configuring and verifying configuration
- Maintenance of security

Establishing Baseline Requirements

References Reputable sources were studied to establish the baseline requirements—the essentials for a secure NT4.0/IIS4.0 system—as well as past experience with IIS3.0. The sources include: Microsoft Internet Information Server 4.0 Security Checklist (Last updated 15-Mar-2000), from the Microsoft TechNet security web site; the Microsoft TechNet white paper "Designing and Planning Windows NT External Security", by Microsoft Consulting Services, Southern California; numerous Microsoft Knowledge Base articles; and the SANS Institute DC2000 course and materials on NT and IIS security.

Software The first requirement is that the software complement be known and tightly controlled. NT must be installed from scratch using only NTFS filesystem as a stand alone server, then IIS according to the sequence recommended in the Microsoft Knowledge Base: SP3 or later, IE4.0 SP2, NT Option Pack (default except no Index Server, no Front Page server extensions, and plus Site Server Express), then MDAC 2.1, Microsoft Security Configuration Manager, then SP6a, followed by Oracle Client (minimal components needed) 8.05, VBScripting Engine 5.1, tnsnames.ora file (only

minimal information included), PC Anywhere 9.2 Host Only, and local MTS packages, DLL's and ActiveX.

On this base platform a selection of relevant post-SP6a hotfixes is applied, in order of the date of the release of the executable file:

Hotfixes Selected Post SP6a Hotfixes Release Dates --Applied in sequence of release dates 7/27/2000

escseq4i.exe unknown -- not applied

q259496i.exe 16 Nov 1999 C-2 config --applied 7/27/2000

uncsec4i.exe 24 Feb 2000 UNC shares --applied 7/27/2000

chkenc4i.exe 20 Mar 2000 Chunk Encoding --applied 7/27/2000

q244599i.exe 12 Apr 2000 Offload Mod Expo --applied 7/27/2000

q259622i.exe 20 Apr 2000 Malformed Environment Variable --applied 7/27/2000

q259728i.exe 8 May 2000 IP Fragment Reassembly --applied 7/27/2000

myrdot4i.exe 11 May 2000 Malformed Extensions in URL --applied 7/27/2000

MS00-025 Front Page server extension buffer overrun. Recommended action is file deletion. dvwssr.dll not found --7/27/2000

MS00-028 Front Page Server Extension buffer overrun. Recommended action is file deletion.

c:\Inetpub\wwwroot\cgi-bin_vti_cnf\Htimage.exe, imagemap.exe deleted 7/27/2000

A record should exist of hotfixes applied; if this becomes infeasible, third-party analysis tools could be used to verify the status of a system.

Microsoft's Security Configuration Manager/Editior, backported from Windows 2000 and new in NT 4.0 SP4, enables you to consolidate the configuration of many security related settings in one Microsoft Management Console view. This will be used to create a template with the baseline settings for comparison to other installations, as well as for applying the necessary settings. The Security Configuration Manager MMC Snap-In has

multiple bugs in SP4 (KB article Q218934) which can be fixed by applying SP6a. The manager can also be used to save and apply a low security configuration in case crippling occurs (generally shows up when installing new software on hardened machine). Some crippling is useful for operations and is reversible, such as unbinding WINS client from the adapter and disabling the Workstation and Server services. These services are needed to easily update software and to use the User Manager.

The High Security Domain Controller template was copied and modified to establish a NYSIF template. In the MMC, a right click on the Configurations object gives you options to extend the template, for instance adding new folders and files for NTFS ACL's or registry keys for ACL's. In "File and Registry Object Configuration", you can select whether an object's template settings override host settings or are ignored.

NTFS ACLs can be applied by the SCM. The following rules were set up, based on the MCS white paper and SANS course. It is necessary to avoid crippling permissions which could cause future software installation to fail.

Path	Rights
%SYSTEMROOT%	Administrators:F CREATOR OWNER:F Everyone:R SYSTEM:F
%SYSTEMROOT%\REPAIR	Administrators:F
%SYSTEMROOT%\SYSTEM32\CONFIG	Administrators:F CREATOR OWNER:F Everyone:List SYSTEM:F
%SYSTEMROOT%\SYSTEM32\SPOOL %SYSTEMROOT%\SYSTEM32\SPOOL\PRINTERS	Administrators:F CREATOR OWNER: F Everyone:R SYSTEM:F
%SYSTEMROOT%\Cookies (added to generic template) %SYSTEMROOT%\Downloaded Program Files (not present on host)	No sharing Administrators:C System:F

%SYSTEMROOT%\History %SYSTEMROOT%\Subscriptions %SYSTEMROOT%\Temporary Internet Files %SYSTEMROOT%\WEB	
\BOOT.INI \NTDETECT.COM \NTLDR	Administrators:F System:F Everyone:R
\AUTOEXEC.BAT \CONFIG.SYS	Administrators:F SYSTEM:F Everyone:R
\TEMP directory	Administrators:F CREATOR OWNER:F Everyone:Modify SYSTEM:F
%systemroot%\system32\Logfiles and subdirectories	Administrators, SYSTEM:F, Authenticated Users:List.
%SYSTEMROOT%\System32\Inetsrv\Metabase.bin	Administrators, SYSTEM:Full
PC Anywhere program files	Administrators, System: Full
%SYSTEMROOT%\SYSTEM32\Inetsrv\MetaBack	Administrators, System:Full. Audit all failed access to this folder.
C:\CommonTools, C:\I386, C:\SP5, C:\backup	Administrators:R
C:\Dell	Adminstrators: F, System:Full
C:\Inetpub\ftproot	Administrators,System:F,

	Creator Owner:Modify Authenticated Uses: Modify Audit failed access

Registry Settings. Numerous registry settings are used to turn off features that make intrusion easier. Registry settings also need ACL's. The ACL's can be set in the template (the generic template included 71). Some security related registry keys appear as template options, with text descriptions, under Local Policies/Security Options. Most of the high security template registry ACL's allow Authenticated Users only RX rights (25 entries). Many of these entries had Account Unknown, probably due to the renaming of the Administrator account; for these, Account Unknown was removed, Administrators and System given Full control, Creator/Owner Change.

Hive
HKEY_LOCAL_MACHINE\SYSTEM
Key
\CurrentControlSet\Control\FileSystem
Name
NtfsDisable8dot3NameCreation
Type
REG_DWORD
Value
1
(Turn off 8.3 filename generation.) Use REGEDT32.

Hive	HKEY_LOCAL_MACHINE\SOFTWARE
Key	\Microsoft\OS/2 Subsystem for NT
Action	Delete all sub keys

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	\CurrentControlSet\Control\Session Manager\Environment
Name	Os2LibPath
Action	Delete

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	\CurrentControlSet\Control\Session Manager\SubSystems
Name	Optional
Action	Delete values

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	\CurrentControlSet\Control\Session Manager\SubSystems
Action	Delete entries for Posix and OS/2

Here it is also necessary to delete the \winnt\system32\os2 directory and subdirectories. (Removes OS/2 and Posix subsystems). Use REGEDT32 and Windows Explorer.

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	CurrentControlSet\Services\LanmanServer\Parameters

Name	AutoShareServer
Type	REG_DWORD
Value	0

(Remove Administrative Shares). Use REGEDT32.

Hive	HKEY_LOCAL_MACHINE\SOFTWARE
Key	\Microsoft\Windows NT\Current Version\Winlogon
Name	DontDisplayLastUserName
Type	REG_SZ
Value	1

(Hide last logon user name). (in template).

Hive	HKEY_LOCAL_MACHINE\SOFTWARE
Key	\Microsoft\Windows NT\Current Version\Winlogon
Name	LegalNoticeCaption
Type	REG_SZ
Value	NYSIF Authorized Users Only

Hive	HKEY_LOCAL_MACHINE\SOFTWARE
Key	Microsoft\Windows NT\Current Version\Winlogon
Name	LegalNoticeText
Type	REG_SZ
Value	Unauthorized Use Will Be Monitored and Prosecuted

(Preserve legal right to monitor intruders.) (in template).

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	\CurrentControlSet\Control\SecurePipeServers
Name	\winreg

(ACL this key to limit remote access to the registry (Administrators:R, SYSTEM:F).). in template.

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	CurrentControlSet\Control\LSA
Name	RestrictAnonymous
Type	REG_DWORD
Value	1

(Block null user access to user list) In template.

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	CurrentControlSet\Control\LSA
Name	NotificationPackages
Type	REG_MULTI_SZ
Value	FPNWCLNT PASSFILT

(Enable Password filtering; requires copying PASSFILT.DLL to %SYSTEMROOT%\SYSTEM32 and ACL'ing it to prevent trojan password filters).
(ACL this key-Read Only to prevent trojan password filters)

References: Microsoft white paper p.28, SANS DC2000 NT p. 101). The LSA key and subkeys were also selected for auditing, to audit Failed access (full control) for Everyone. Can't view auditing details in REGEDT32 after setting in SCM.

Hive	HKEY_LOCAL_MACHINE\SOFTWARE
Key	Microsoft\Windows\CurrentVersion\Run
Hive	HKEY_LOCAL_MACHINE\SOFTWARE
Key	Microsoft\Windows\CurrentVersion\RunOnce
Hive	HKEY_LOCAL_MACHINE\SOFTWARE
Key	Microsoft\Windows\CurrentVersion\RunOnceEx
Hive	HKEY_LOCAL_MACHINE\SOFTWARE
Key	Microsoft\Windows NT\CurrentVersion\AeDebug
Hive	HKEY_LOCAL_MACHINE\SOFTWARE
Key	Microsoft\Windows NT\CurrentVersion\WinLogon

(ACL these keys to prevent trojan programs from being launched:

The default ACLs should be:

- Administrators (Full Control)

- SYSTEM (Full Control)

- Creator Owner (Full Owner)

- Authenticated Users (R))

- These keys were also selected for auditing, audit Everyone for success and failure, full control. That is in the template too.

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	CurrentControlSet\Services\W3SVC\Parameters
Name	SSIEnableCmdDirective
Type	REG_DWORD
Value	0

(Disables feature allowing command shell calls from HTML pages) Use REGEDT32.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
W3SVC\Parameters\ADCLaunch\VbBusObj.VbBusObjCls

(Disable RDS support. RDS Datafactory enables client based SQL queries to OLE DB data sources on the web server. Known security hole, Knowledge Base article Q184375. Remove these registry keys and any subkeys) Use REGEDT32.

System Policy These options are contained in the security template, in greater detail. The Server Operators group was removed because it only applies on domain controllers.

Password Length: 9 character minimum.

Windows NT User Rights (again to secure without crippling):

Log On Locally	Administrators and IUSR_ and IWAM_ Backup Operators
Shut down the system	Administrators
Access this computer from the network	Administrators, and IUSR_ and IWAM_
Act as part of the operating system	NONE
Add workstations to the domain	NONE
Back up files and directories	Administrators Backup Operators
Bypass traverse checking	Everyone
Change the system time	Administrators
Create a pagefile	Administrators
Create a token object	NONE
Create permananent shared objects	NONE
Debug programs	Administrators
Force shutdown from a remote system	Administrators
Generate security audits	NONE
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	NONE
Log on as a batch job	NONE
Log on as a service	NONE

Manage auditing and security log	Administrators
Modify firmware environment variables	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Replace a process level token	NONE
Restore files and directories	Administrators Backup Operators
Take ownership of files or objects	Administrators

Audit Policy. Also set in template, by slightly different names.

Event	**Success**	**Failure**
Logon and Logoff	X	X
File and Object Access		X
Use of User Rights		
User and Group Management (Account Management)	X	X
Security Policy Changes	X	X
Restart, Shutdown (System Events)	X	X
Process Tracking		

Log Settings. Also in template. Max Log Size, 20032 K (to nearest 64K); Event log wrapping, Overwrite Events older than 14 days.

Users and Groups. Guest account is disabled. Administrator is copied, renamed, given a very strong password; a dummy Administrator account with no group memberships is created with a weak password. Use USER MANAGER FOR DOMAINS.

Group Membership can be checked in the SCM: The only other accounts are the IUSR_computername and IWAM_computername accounts. Local Group membership:

Administrators contains only the renamed Administrator account.

Backup Operators, Replicator have no members.

NT Security Enhancements. Microsoft has released and recommends several enhancements:

SYSKEY encrypts the SAM database. Select the option to keep the encryption key on the machine. An rdisk /s ERD will be needed to boot up if the database cannot be decrypted. (SP3)

Passprop /adminlockout /complex (NTReskit) enables lockout of the administrator account (except at the console)

Common Tools. Microsoft recommends moving common administrative tools to a separate directory and ACL'ing them. Here is a batch file to do it, to be run against the system32 and winnt directories:

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

In \CommonTools, the ACL is set to allow only Read access, only to Administrators.

Also, check the FPNWCLNT and PASSFILT DLL (To Enable Password filtering; requires copying PASSFILT.DLL to %SYSTEMROOT%\SYSTEM32 and ACL'ing it to prevent trojan password filters, as well as registry changes previously indicated).

IIS Specific Settings

Run only these necessary services and disable the rest (in Template):

- Event Log
- License Logging Service
- Windows NTLM Security Support Provider
- Remote Procedure Call (RPC) Service
- IIS Admin Service
- MSDTC (Distributed Transaction Coordinator
- World Wide Web Publishing Service
- Protected Storage

The Server Service will be needed to run User manager. (SANS DC2000 Track 5.4 Internet Information Server, p. 54) but disable it in normal operation.

The SCM also allows setting security on how to run services.

Virtual directory NTFS Permissions. Administrator, System: Full, IUSR_ and IWAM_, Read. Use ACL inheritance (requres Security Configuration Editor installed) and verify that it is working as you expect.

All directory trees were given ACL's in the template, including downloaded software, hotfixes, service packs, etc. restricting them to Administrator access.

W3C Extended Logging attributes: in MMC, include:

- Client IP Address
- User name
- Method
- URI stem

- HTTP status
- User Agent
- Server IP Address
- Server Port

SSL: Each web app should have a Secure folder within its tree to place SSL pages, in case any data flowing to or from the script is confidential. In MMC, under Directory Security for the folder, check Require Secure Connection.

Sample Applications: IISADMPWD virtual directory, iissamples (c:\inetpub\iissamples), iis sdk (c:\inetpub\iissamples\sdk), c:\inetpub\Adminscripts, and c:\Program files\Common Files\System\msdac\Samples should be removed from the filesystem and their virtual counterparts in MMC.

Directory locations. Root virtual folders will not be placed on the system partition, nor will log files. D:\errorlogs folder and FroiErrors.log files must be created.

Unused Script Mappings: In MMC under Home Directory and Configuration for the application space, remove script mappings except .asp and .pl (if needed).

File System Object: Cannot Unregister scrrun.dll: regsvr32 scrrun.dll /u, it would break application error logging.

Disable Parent Paths: in MMC under Home Directory | Configuration | App options.

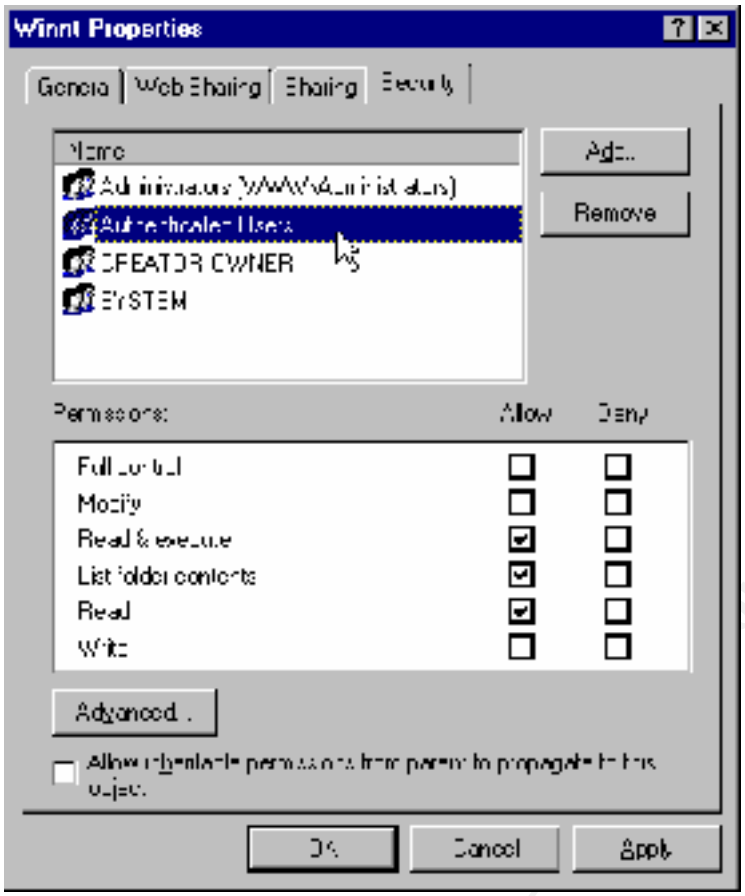
Input testing: ASP pages must use regular expressions on server side to test input for valid characters and length, or embedded commands.

Index Server is not be installed.

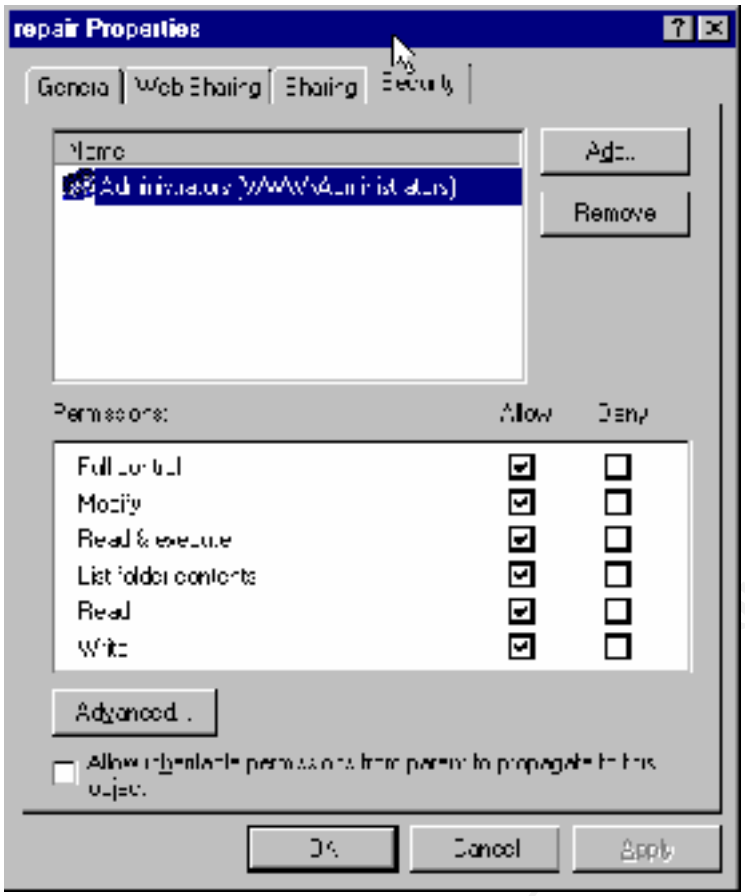
Methods of Configuring and Verifying Conformance

Many of the baseline settings described are configurable in one of several NT4.0 administrative tools; however, a significant portion of these can be consolidated in a single view in the Security Configuration Manager. The settings can be saved as a group in a security template, which can be applied and verified in the Microsoft Management Console.

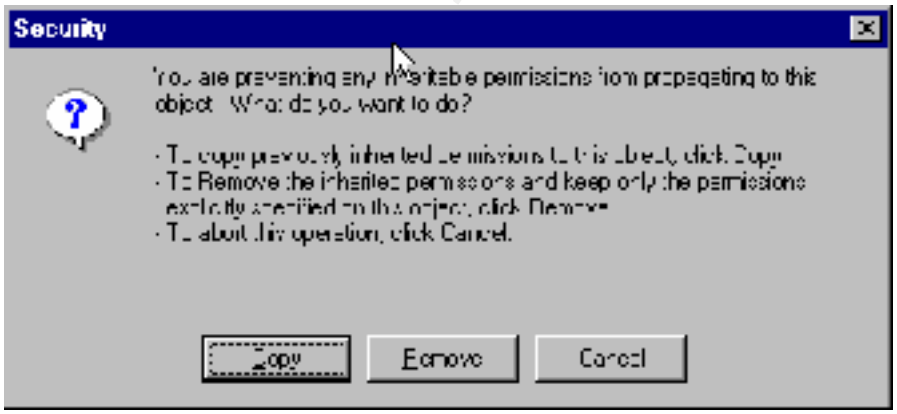
Tool by tool method. Here are examples:



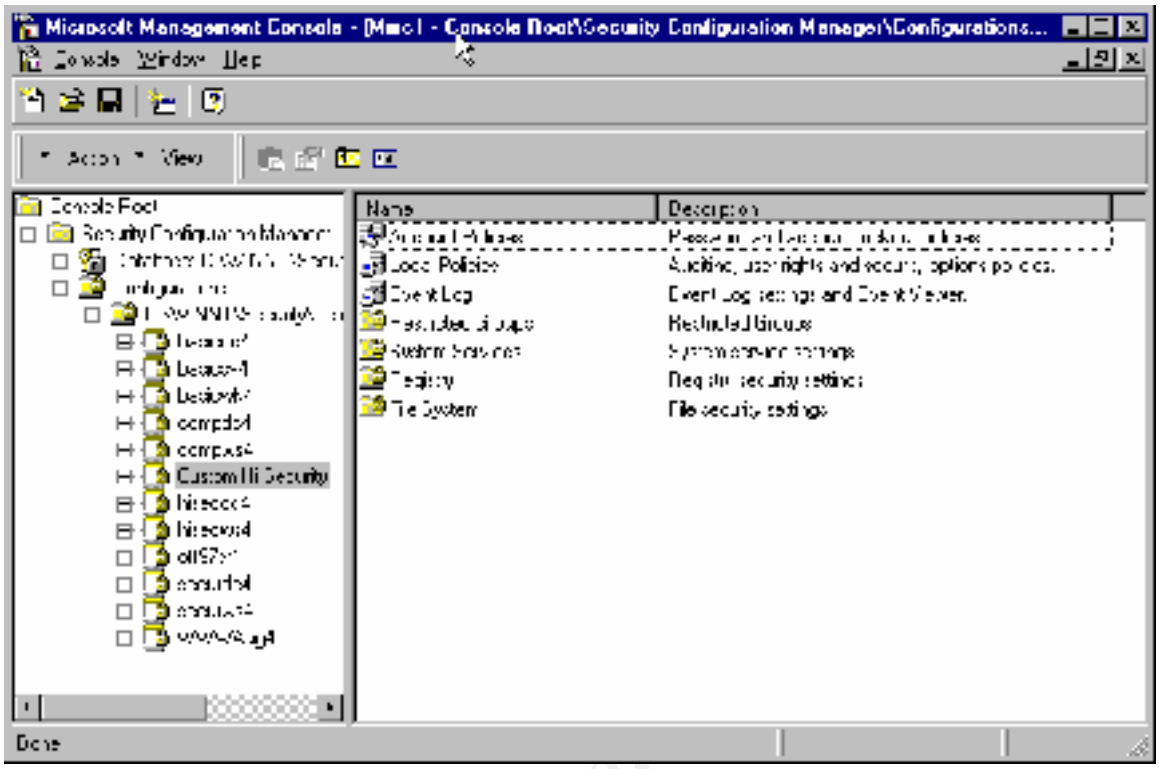
Here the Winnt directory permissions are being restricted; Everyone has been removed, and Authenticated Users allowed Read, Execute, and List. The Explorer dialog is changed by the installation of the SCM.



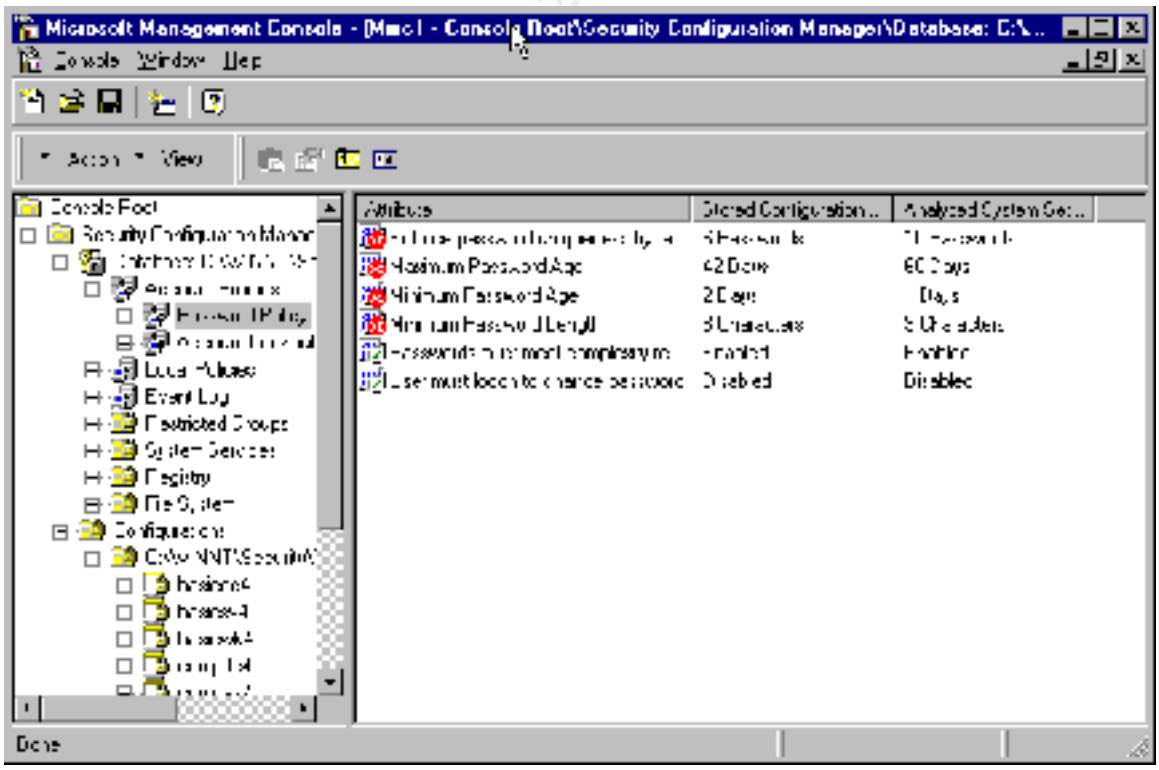
Here the repair directory is being restricted to Administrators (it can contain a copy of the SAM database).



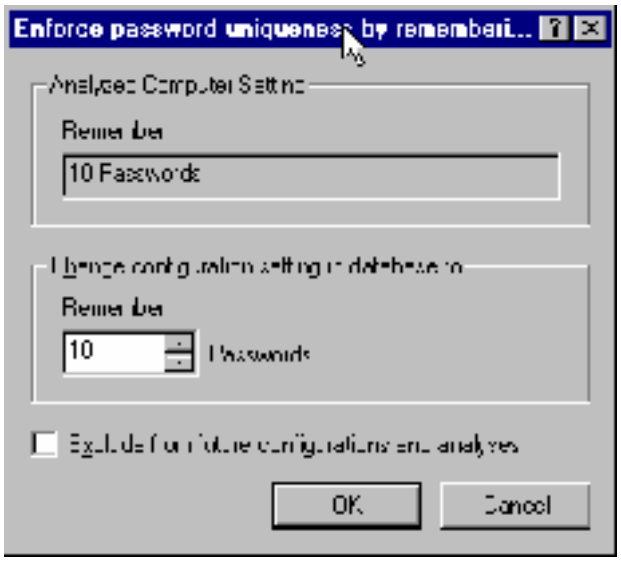
The Explorer with SCM is asking you to specify the inheritance of ACL's to subfolders.



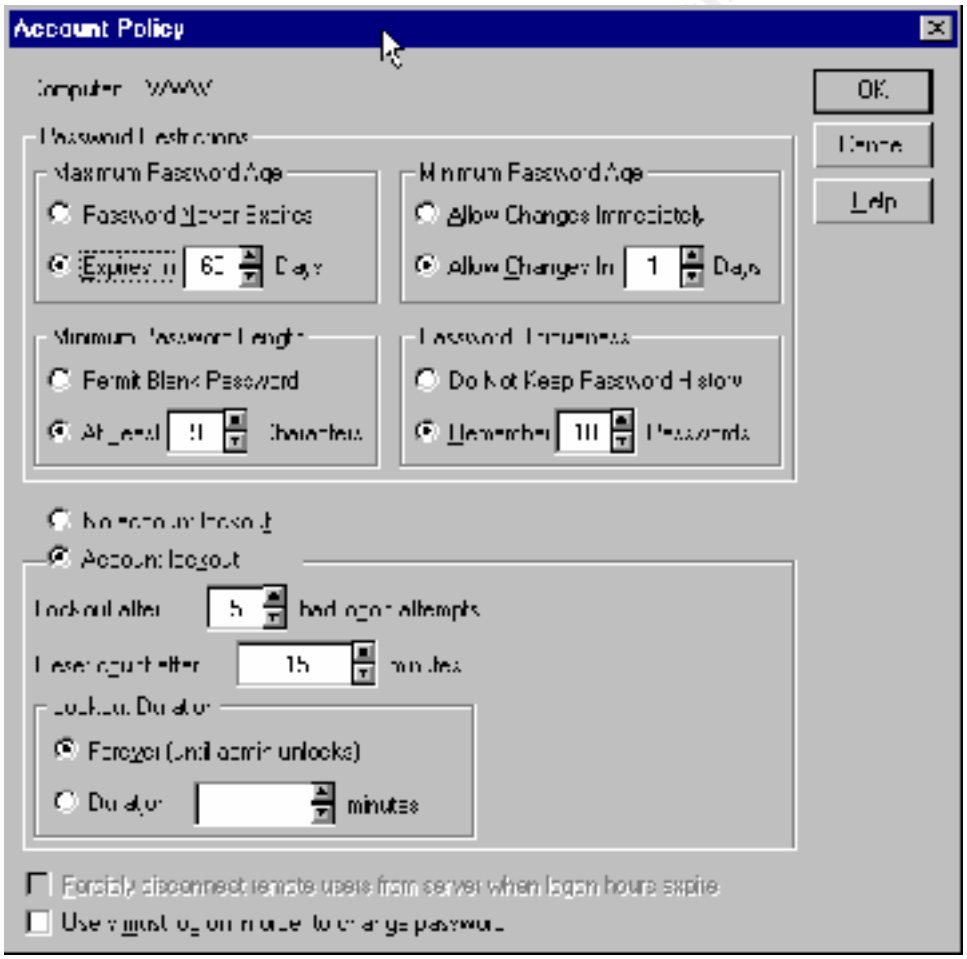
The SCE, with its default templates.



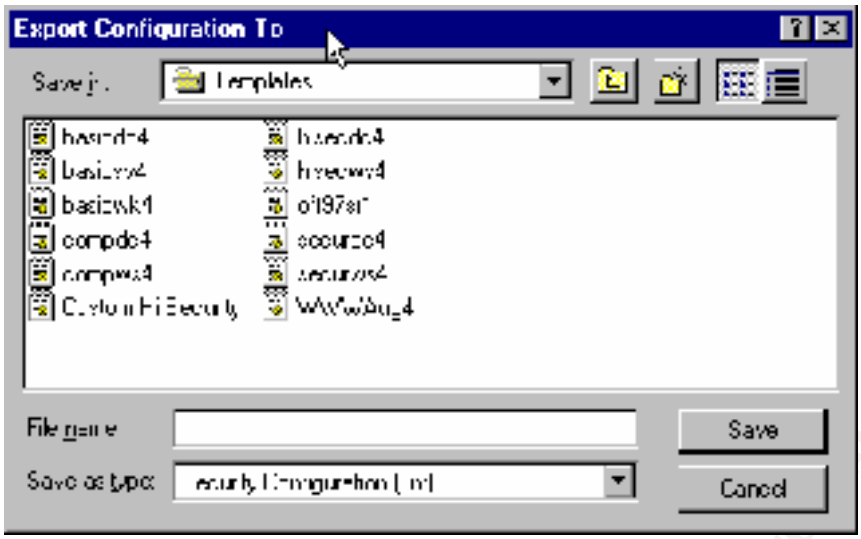
SCE showing mismatches with the current template.



SCE dialog to modify the template.



Account policy tool showing change made by SCE.



Dialog to save template in SCE.

The illustrated methods can be used to build necessary templates and use them.

Maintenance of Security

Security is an ongoing process. New vulnerabilities will be tracked by the Microsoft security mailing list, Ntbugtraq.com, Microsoft Technet Security website, SANS bulletins, CERT advisories mailing list. New service packs and hotfixes must be examined as they come out.

Because stealthy intrusions are possible, intrusion detection and monitoring by Tripwire will be implemented. Automated log analyzers will be investigated for possible use. Host availability will be monitored with IPSentry.

Recovery procedures will also be part of the plan. We will Ghost the server, and keep tape backups, as well as a fully configured spare/test server.

Several known hacker targets in the registry and filesystem are audited for use as honeypots to detect intrusion attempts.

Netcat will be used to do port scanning of internal hosts from the web server to detect vulnerabilities.

We will unbind the WINS client from the adapter in normal operation to avoid any possible Microsoft networking vulnerability.