Global Information Assurance Certification Paper

Baseline Security for Windows NT and 2000 Servers

By Craig Larscheid

Table of Contents

1. Introduction

Regardless of the use or location of a Windows NT or 2000 Server, there is a baseline of hardening items that need to be addressed across the board to secure a freshly installed operating system. Microsoft has put a great deal of emphasis on producing a server operating system that is easily configured, plays well with 3rd party applications, and creates little or no headaches for administrators. "Easily configured" and "no headaches", however, usually imply loose restrictions that need hardening. This does indeed seem to be the case with Microsoft, as illustrated in a Microsoft Certified

Professional Magazine article from October 19, 2002. In the article, "Microsoft Says Security Emphasis is Paradigm Shift" [1], author Matt Migliore writes about comments made by Microsoft senior vice president for Windows, Brian Valentine, 'With previous versions of Windows Server, Valentine said security wasn't a primary concern. "Originally, the focus was getting people on the network, not keeping people off it."'

The ability to quickly deploy Microsoft Server solutions does indeed have its merit, but obviously has detracted from the security of the OS. With this in mind, the scope of this paper is centered on hardening Windows NT and 2000 base server operating systems after installation, and avoiding the opening of new holes. It will be assumed that the audience is familiar with Windows Server installation and administration.

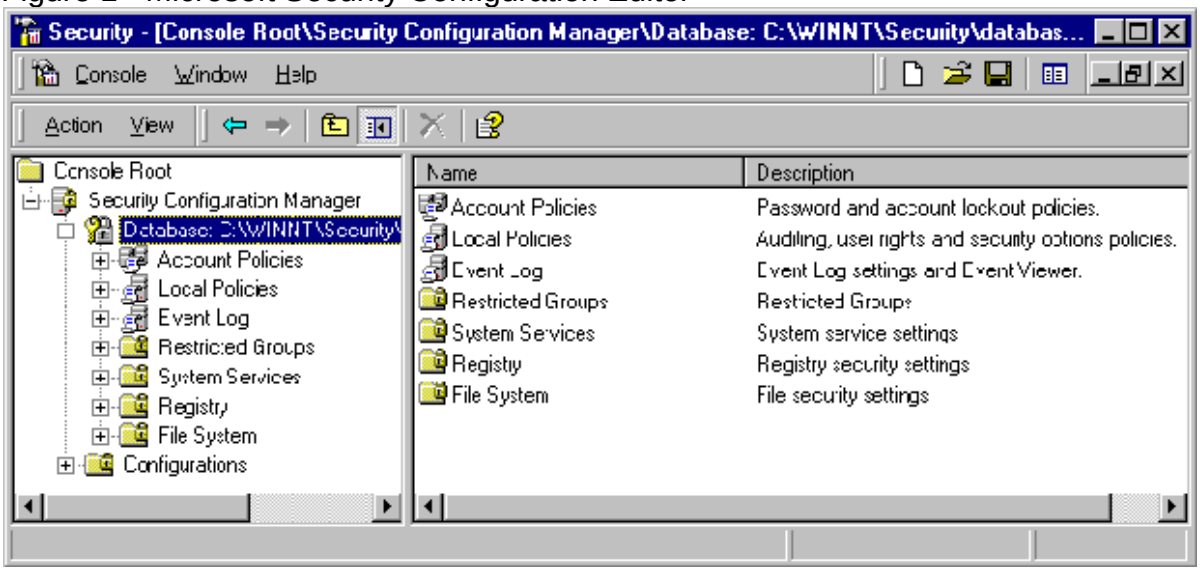
2. Tools

The tools that will be utilized in configuring the Windows Servers to a hardened baseline are:

Microsoft Security Configuration Editor (Windows NT 4.0 - Figure 1 below) -

Service Pack 4 includes the Microsoft Security Configuration Editor. This tool allows administrators to combine security related system settings for Account Policies, Local Policies, the Event Log, Group Member Control, the System Registry, and the File System into a single configuration file which can then be applied to the server. The tool also contains sample policies which can be modified for different security environments.

Figure 1 - Microsoft Security Configuration Editor

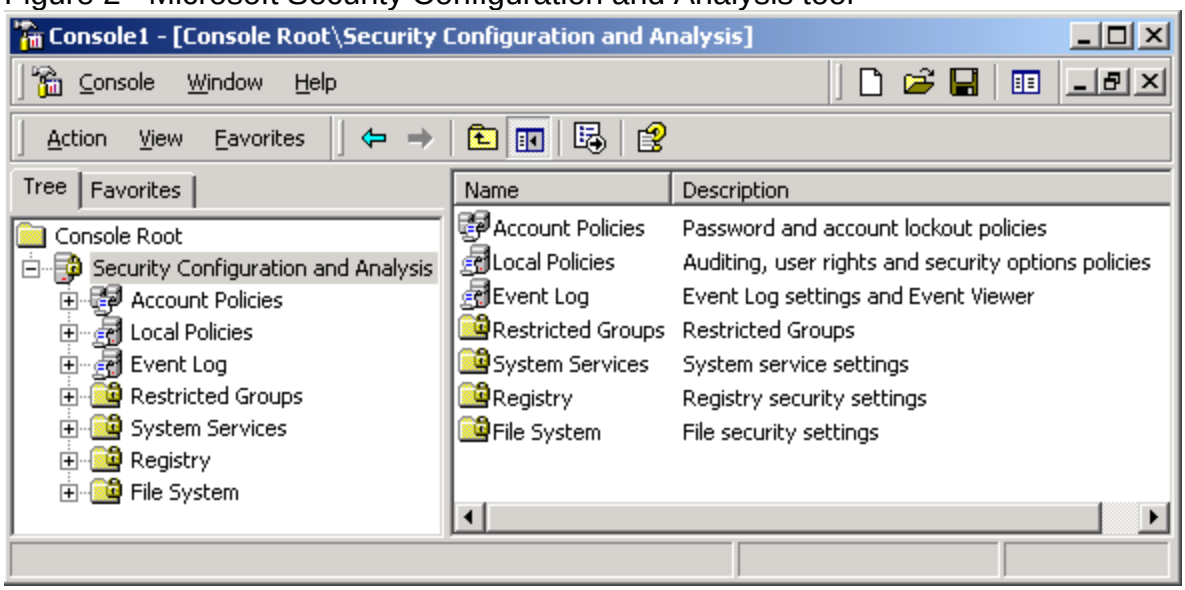


Microsoft Security Configuration and Analysis tool (Windows 2000 - Figure 2 below) -

This tool, like the Security Configuration Editor for Windows NT, also allows administrators to combine security related system settings for Account Policies, Local Policies, Event Log Settings, Group Member Control, System Registry

Settings, and the File System settings into a single configuration file which can then be applied to the server. The tool also contains sample policies that can be modified for different security environments.

Figure 2 - Microsoft Security Configuration and Analysis tool



Highlights of the configuration areas for both tools are as follows;

Account Policies –

Password Policy – Key areas to enforce for an effective password policy are; password history, minimum and maximum password age, minimum password length and complexity requirements.

Account Lockout Policy - Lockout threshold, lockout duration and reset account lockout counter have to be enforced to restrict attackers from brute force password attacks.

Local Policies –

Audit Policy – Most corporate audit policies will require at least tracking failure audits for most of the settings in the tool. Common success auditing would be for account logon events, account management, policy change, privilege use, and system events. Care should be taken when deciding which areas to audit. Successful object access, for example, could possibly fill up event logs fairly quickly.

User Rights Assignment – User rights assignments should only be granted on a least privilege basis. Similarly, if service accounts are necessary for commercial applications, grant only the service account the privilege, rather than an entire group. An example would be a service account needing to be part of the Administrators group, but also needing logon as a service, logon as a batch job and act as part of the operating system user rights. Operating with least privilege in mind, grant only the service

account the user rights above rather than the entire Administrators group.

Security Options – Common areas to restrict include; restrictions for anonymous connections (usually no reason to allow anonymous enumeration of users and shares), allow system to be shut down without having to log on, amount of idle time required before disconnecting session, LAN manager authentication level (disallow LAN manager if possible), restrict CD-ROM access to locally logged-on user only, and restrict floppy access to locally logged-on user only. Common areas to configure include; amount of idle time required before disconnecting session, audit use of backup and restore privilege, do not display last user name in logon screen, message text for users attempting to log on (might be difficult to persecute someone for a computer security breach if no warning saying not to do so, and stating legal consequences), message title for users attempting to log on, number of previous logons to cache (in environments where availability is a concern, cached logons might be useful if local accounts are locked out and domain is not available), prompt user to change password before expiration, rename administrator account, rename guest account, unsigned driver installation behavior, and unsigned non-driver installation behavior. Be cautious with the following settings; clear virtual memory pagefile when system shuts down (in environments where uptime is crucial, and where servers have large amounts of memory, servers might take a long time to reboot), digitally sign client communications (always), digitally sign server communication (always), secure channel: digitally encrypt or sign secure channel data (always), secure channel: require strong (Windows 2000 or later) session key, and shut down system immediately if unable to log security audits (this setting could possibly create a denial of service).

Event Log –

Settings for Event Logs – The key areas for event logs are; setting the appropriate log sizes, restricting guest access to logs (usually not a reason to enable a guest to read logs), and log retention and method. Most corporate security policies dictate the retention period for security logs.

Restricted Groups –

Allows the ability to restrict membership in built-in groups such as Administrators, Server Operators, Power Users, etc… For example, to limit membership in the Domain Administrators group, specify the allowed members in the template.

System Services –

Allows the ability to define startup parameters for services; Automatic, Manual, and Disabled. In addition, under Edit Security, security can be established as to who has what control of the specific services. For example, if there is a need for a user or group to be able to Start, Stop or Pause a specific service, configure it here.

Registry –

Allows the ability to configure Access Control settings for the Registry, which was typically done with REGEDT32.exe in Windows NT and 2000. Registry auditing can also be implemented in the Advanced Security Settings tab under Auditing.

File System –

Allows the ability to configure Access Control settings for the File System, which was typically done with Windows NT Explorer in Windows NT and 2000. File and Directory auditing can also be implemented in the Advanced Security Settings tab under auditing. Operating with least privilege in mind, ideal settings for securing the file system would be to allow Administrators and System Full Control, and Authenticated users Read and Execute.

Security Checklist

Although the security configuration tools above allow an administrator to modify a wide range of security settings, security checklists and manual intervention are still needed. Table 1 below, will assist in documenting security configuration items that are not covered by a security template or policy, need second checking, and/or which need to be manually remedied. Batch files can be used to automate the application of several manual fixes into one (for example, file deletions and registry changes can be implemented with the use of Resource Kit utilities via batch files. Please see examples in the Server Security Checklist below).

Additional resources for establishing a security baseline are;

- Windows NT 4.0 Server Baseline Security Checklist – Windows NT [2]
- Windows 2000 Server Baseline Security Checklist - Windows 2000 [3]

Server Security Checklist

	Items to be remedied manually
	Create Emergency Repair Disk To be updated every 6 months and stored in a secure location, readily accessible to administration staff. *Start / Run / Rdisk for Windows NT, or Start / Programs / Accessories / System Tools / Backup / Emergency Repair Disk for Windows 2000
	All volumes on server must use NTFS. *Right click on partition in Explorer / select Properties / General Tab and see if partition is NTFS. Convert.exe can be run to convert FAT and FAT32 file systems to NTFS.

	Enable PASSPROP with /adminlockout and /complex variables. For NT, this NT Resource Kit utility forces passwords to have a mixture of upper and lower-case characters, symbols and numbers. For Windows 2000 complex passwords can be implemented with a security template in the Account Policies / Password Policy area.
	Remove registry keys and/or files for DOS, Posix, OS/2 or other secondary operating systems. WARNING: Removal of Win16 subsystem will prevent some applications from running. Example for batch file creation; cd %systemroot%\system32 rd %systemroot%\system32\os2 /s /q del %systemroot%\system32\os2.exe /s del %systemroot%\system32\os2srv.exe /s del %systemroot%\system32\os2ss.exe /s del %systemroot%\system32\posix.exe /s del %systemroot%\system32\psxdll.dll /s del %systemroot%\system32\psxss.exe /s
	Remove all unnecessary or undocumented shares All shares must have up-to-date documentation on file with the system administration staff that includes purpose and contents of the share and permissions required. Administrative shares (C$, D$, etc…) can be removed by changing the following registry key to a value of "0": HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\autoshareserver
	Remove all unnecessary or undocumented scheduled tasks. All scheduled tasks must have up-to-date documentation on file with the system administration staff that includes purpose of the task and location of scripts and other executables associated with the task. To view scheduled tasks, type "at" in a command prompt window. If scheduling jobs is not required, the Scheduler Service (NT) or Task Scheduler Service (Win2k) should be disabled.
	Disallow anonymous enumeration of shares, and users. Registry key value of "1" should be implemented on the following key to disallow anonymous enumeration: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RestrictAnonymous
	Disallow anonymous methods of access to the file system, including anonymous FTP and TFTP.
	Verify that time synchronization is properly and uniformly configured.

	Resource Kit Utility Timeserv.exe can be used for time synchronization, as well as Network Time Protocol client synchronization with an NTP server if available.
	If MDAC is present, verify that it is the most current version for the OS. Check http://windowsupdate.microsoft.com for updates to MDAC, as well as http://www.microsoft.com/technet/security for security related hotfixes.
	Remove files - RCP.EXE,REXEC.EXE,RSH.EXE,RLOGIN.EXE Example for batch file creation; del %systemroot%\system32\rcp.exe /s del %systemroot%\system32\rexec.exe /s del %systemroot%\system32\rsh.exe /s del %systemroot%\system32\rlogin.exe /s
	For each system that requires SNMP, use the SNMP control panel to change the community string from the default and to only allow connections to/from legitimate SNMP hosts. *Default communities and new settings can also be changed or implemented with the usage of the Resource Kit Utility “Reg.exe”. For example; reg delete hklm\system\currentcontrolset\services\snmp\parameters\trapconfiguration\admin /force reg delete hklm\system\currentcontrolset\services\snmp\parameters\trapconfiguration\public /force reg delete hklm\system\currentcontrolset\services\snmp\parameters\validcommunities\admin /force reg delete hklm\system\currentcontrolset\services\snmp\parameters\validcommunities\public /force
	Rename Administrator and Guest accounts. ??Accounts can be renamed with a security template under Local Policies / Security Options.
	Verify that all service packs and hotfixes, that have been shown to not adversely affect system availability, have been applied. Depending on the environment and corporate policy, patches can be downloaded and applied at once by visiting http://windowsupdate.microsoft.com or downloaded to a centralized location for future controlled deployment at http://corporate.windowsupdate.microsoft.com.
	All Run/RunOnce/RunOnceEx entries in the registry are to be approved by the System Administration and Operations Security staff and documented. Registry keys to check are; HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx

3. Building the server

During the build of the OS, several items need to be addressed:

Avoid installing, or disable after installation, unnecessary components or services. Similarly, install only the necessary network protocol/s (TCP/IP for example). Following is a list of services that are unnecessary in most environments (please see Table 2 in the Appendix for an example of disabling services by using the Microsoft Security Configuration and Analysis tool);

1.) Alerter - Notifies selected users and computers of administrative alerts that occur on a computer.
2.) Browser - Provides a list of shared resources on a network
3.) Messenger - Sends and receives messages sent by administrators or the Alerter service
4.) Schedule - Allows executables to be scheduled and started at specific times.
5.) Clipbook Server - Allows local clipboard to be shared over the network.
6.) Dynamic Host Configuration Protocol (DHCP) Client - Automatically obtains an IP address from the DHCP server.
7.) Spooler - Provides print services.
8.) Telephony Service - Provides advanced phone services.
9.) Remote Procedure Calls (RPC) Locator - Allows distributed applications to use the RPC Name service.
10.) Server - Provides file and print sharing (See Note)

Note:
The Server service provides:

- File and print sharing
- Drive mapping
- Remote access to Win2k resources via MMC (event log, local users and groups)
- Creation of administrative shares (C$)

Avoid performing a "default" installation of the OS or any add on package such as IIS. Special care needs to be taken in selecting which portion of the OS or packages need to be installed. A default installation of IIS 4.0 on an NT 4.0 server, for instance, installed the Remote Data Service (RDS) which, when unpatched, could allow unauthorized access by Internet users (4).

Utilize NTFS for all partitions. There is no way to secure the file system of a server with FAT partitions. In addition, once new partitions are created, immediately go into the NTFS security properties, and change the default Everyone Full Control to Authenticated Users Read and Execute, System Full Control and Administrators Full Control.

Apply all appropriate patches. After the OS is built, install the latest service packs and patches for all components of the server, web browser, applications, and OS. Patches can be automatically downloaded and installed for all Windows components from http://windowsupdate.microsoft.com , or downloaded for a controlled installation at either http://corporate.windowsupdate.microsoft.com or http://microsoft.com/technet/security . Patches and service packs are routinely provided to resolve security vulnerabilities, program fixes and enhancements. After the last patch is installed and the server is rebooted, it is time to harden the OS.

4. Hardening the server

Now that the OS is up and running with minimal services and protocols, NTFS partitions, and current patch levels, it is time to harden the server using the security configuration tool for the appropriate server. For NT servers, the Security Configuration Editor has to be downloaded and installed before applying a policy. Windows 2000 servers, on the other hand, are ready to go since the Microsoft Security Configuration and Analysis tool just needs to be added to an MMC. Both tools, however, utilize the same type of configuration file to obtain the security settings that need to be applied to the server (See Figure 3 in the Appendix). The supplied sample policy, which is found after installation in the %systemroot%\Security\Templates directory, was derived from the default high security Microsoft Windows NT 4.0 Domain Controller "hisecdc4.inf" policy. (Policy has been precisely edited to work in author's environment and comply with local security policies. Policy has been installed on numerous production Domain Controllers, but no guarantees are given or are being implied).

Highlights of SampleHighSecurityPolicy.inf:

- File System and Registry Security have been hardened to what Microsoft recommends for high security servers (hisecdc4.inf).
- Anonymous, or null session access, is prohibited in the [Registry] section.
- The Everyone Group has been stripped of all privileges except where Microsoft deemed it necessary in a high security environment.

CAUTION: All policies need to be carefully developed, configuration item by configuration item, and then tested in a non-production environment prior to production rollout. Also, there are settings in the default NT 4.0 policies, hisecdc4.inf and hisecws4.inf, that disable normal server to domain controller communication in an NT 4.0 domain.

This configuration policy, from Figure 3 in the Appendix, allows for the configuration of Account Policies, Local Policies, Event Log Settings, Group Member Control, System Registry Settings, and File System settings. Analyzing this policy file should aid in understanding what these tools are capable of, and what is going to happen to the server once the policy is imported into the server's configuration. Two of the most important areas of configuration are System Registry and File System ACL settings. NT 4.0 and Windows 2000 both allow the Everyone Group access to areas where the group should not exist. For example, in Windows 2000, the Everyone Group by default has Full Control privileges on the %system root% folder, as well as Full Control of all new partitions and shares! Since the Windows 2000 file system has an

inheritance model, this configuration propagates to subordinate directories. This default configuration has now opened the door for Trojans, as evidenced by Microsoft Security Bulletin MS02-064 [4], where Microsoft reveals,

> On Windows 2000, the default permissions provide the Everyone group with Full access (Everyone:F) on the system root folder (typically, C:\). In most cases, the system root is not in the search path. However, under certain conditions - for instance, during logon or when applications are invoked directly from the Windows desktop via Start | Run - it can be.
>
> This situation gives rise to a scenario that could enable an attacker to mount a Trojan horse attack against other users of the same system, by creating a program in the system root with the same name as some commonly used program, then waiting for another user to subsequently log onto the system and invoke the program. The Trojan horse program would execute with the user's own privileges, thereby enabling it to take any action that the user could take.

CAUTION: Great caution should be used when applying configuration policies that modify the ACL settings of the file system. Please use the following Microsoft Knowledge Base articles as references regarding default ACL settings for NT and 2000 servers:

Q148437 [5] Default NTFS Permissions in Windows NT

Q244600 [6] Default NTFS Permissions in Windows 2000

Also, if there's a need for restoring default security settings, please refer to Microsoft's solution at - http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/proddocs/SCM_revert.asp. [7]

While dissecting policy and tools is outside of the scope of this paper, a great resource for doing so is Robert Huie's SANS Security Reading Room article - "Security Configuration Tool and Template Settings Usefulness and Shortcomings of the Preconfigured Security Policy Templates that are Included with Windows 2000" [8].

NT 4. 0 Security Configuration Editor and Configuration Policy Installation

Tool Download and Installation - To apply a policy with the Microsoft Security Configuration Editor for NT 4.0, download the tool from Microsoft at http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q195227& [9], then follow the product's Readme.txt file to get system requirements and installation

directions.

Loading the Snap-in - Once the tool is installed, it is time to load the SCE tool into an MMC (Microsoft Management Console). To do so, open an MMC console (%systemroot%\System32\MMC.exe), select Console, then Add/Remove Snap-in, then Add, then select Security Configuration Manager and OK.

Importing a Configuration Policy - Now that the tool is up and running, it is time to import the configuration. To do so, click on Database (which initializes the database that is used for configuration and analysis), then right click on Database and select Import Configuration, and then select the configuration file (make sure to select the "Overwrite existing configuration in database") and open.

Analyzing and/or Configuring System - With the configuration file loaded, it is time to either analyze or configure the system. To do so, right click on Database and select either Analyze or Configure, then enter the name of the log file to be used for dumping the configuration results to, and then OK. Analyze and Configure should be self explanatory - Analyze being the selection for verifying existing security configuration and Configure being the selection to load the configuration settings into the server's configuration.

After the policy has been applied to the server, make sure to check the log file for any errors.

Windows 2000 Security Configuration and Analysis tool setup and Policy Installation

Loading the Snap-in - Open an MMC console (%systemroot%\System32 \MMC.exe), select Console, then Add/Remove Snap-in, then Add, then select Security Configuration and Analysis and OK.

Loading Database and Importing Configuration Policy - Once the Security Configuration and Analysis tool is open, in the console tree, right-click Security Configuration and Analysis and click Open Database. Then, in Open Database, do one of the following:

1. To create a new database, type in a name for the database file and click Open.
2. To open an existing database, select a database and click Open. *If you are creating a new database you must import a configuration policy, and then click Open.

Select the appropriate Error log file and click OK.

Analyzing and/or Configuring System - With the configuration file loaded into the appropriate database, it is time to either analyze or configure the system. To do so, right click on Security Configuration and Analysis and select either Analyze Computer now... or Configure Computer Now..., then enter the name of the log file to be used for dumping the configuration results to, and then OK. Analyze and Configure should be self explanatory - Analyze being the selection for verifying existing security configuration and Configure being the selection to load

the configuration settings into the server's configuration.

After the policy has been applied to the server, make sure to check the log file for any errors.

Checking system settings with security hardening checklist

As a general rule, script anything that can be scripted. Therefore, if settings in the checklist can be implemented within the Microsoft Security Configuration Tool set, add them to the policy. Although the application of the security policy makes the majority of security changes to the OS, there will be times where additional settings need to be verified or changed manually. This is where the security checklist comes in. In Table 1 - Server Security Checklist, all items need to be verified or changed to meet the hardened security baseline configuration. In some environments, a server can't be turned over to developers until the final security checklist is filled out and signed.

After the policy has been applied to the server, make sure to check the log file for any errors.

5. Summary

A carefully configured server has now been built, one with minimal services and protocols, carefully selected components, NTFS partitions, and current patch levels. The server has also been hardened with a policy that contains carefully developed organizationally compliant security configuration settings for Account Policies, Local Policies, the Event Log, Group Member Control, the System Registry, and the File System. Finally, the server was analyzed for compliance with a security checklist. The security checklist helped to second check final system security, as well as point out those items that needed to be manually modified to ensure a standard hardened baseline configuration.

As seen by the amount of configuration still needed to secure a base install of Windows NT or 2000 Server, it seems like Microsoft has a long way to go in developing a secure server operating system that is secure by default. Wouldn't it be nice if Microsoft would come up with an OS that requires Access Control settings to be opened up rather than wide open; services and packages needing to be installed and enabled rather than numerous packages being installed by default and automatically running?

Well, there is good news, as Microsoft is doing just that! The most recent version of the Microsoft Server OS, Windows Server 2003, is reported to be secure right out of the box. Secure right out of the box means administrators can look forward to the following security improvements to the base OS in Windows Server 2003; default Access Control settings for the File System, Registry and shares being based on least privilege, anonymous enumeration of users and shares being prohibited, and only necessary services and packages being installed by default. These 3 steps alone will go a long way in reducing the administrative load required to secure a freshly installed Windows Server operating system.

6. List of Figures and Tables

7. Appendix

[10]

Table 1 - Microsoft Member Server Baseline Policy Service Changes

THIS APPENDIX IS PART OF THE SECURITY OPERATIONS GUIDE FOR WINDOWS 2000 SERVER.
THE DEFAULT COLUMN SHOWS THE SERVICE STARTUP FOR A WINDOWS 2000-BASED SERVER. THE BASELINE COLUMN SHOWS THE CONFIGURED STARTUP FOR EACH SERVICE AFTER THE MEMBER SERVER BASELINE POLICY IS APPLIED.

Service	Full Name	Default	Baseline
Alerter	Alerter	Automatic	Disabled
AppMgmt	Application Management	Manual	Disabled
ClipSrv	ClipBook	Manual	Disabled
EventSystem	COM+ Event System	Manual	Manual
Browser	Computer Browser	Automatic	Disabled
DHCP	DHCP Client	Automatic	Automatic
Dfs	Distributed File System	Automatic	Enabled only in the DC role
TrkWks	Distributed Link Tracking Client	Automatic	Automatic
TrkSrv	Distributed Link Tracking Server	Manual	Disabled
MSDTC	Distributed Transaction Coordinator	Automatic	Disabled
DNSCache	DNS Client	Automatic	Automatic
EventLog	Event Log	Automatic	Automatic
Fax	Fax Service	Manual	Disabled
NtFrs	File Replication	Manual	Disabled
IISADMIN	IIS Admin Service	Automatic	Disabled
Cisvc	Indexing Service	Manual	Disabled
SharedAccess	Internet Connection Sharing	Manual	Disabled
IsmServ	Intersite Messaging	Disabled	Disabled
PolicyAgent	IPSEC Policy Agent (IPSEC Service)	Automatic	Disabled

Kdc	Kerberos Key Distribution Center	Disabled	Enabled only in the DC role
LicenseService	License Logging Service	Automatic	Disabled
Dmserver	Logical Disk Manager	Automatic	Automatic
Dmadmin	Logical Disk Manager Administrative Service	Manual	Manual
Messenger	Messenger	Automatic	Disabled
Netlogon	Net Logon	Automatic*	Automatic
Mnmsrvc	NetMeeting Remote Desktop Sharing	Manual	Disabled
Netman	Network Connections	Manual	Manual
NetDDE	Network DDE	Manual	Disabled
NetDDEdsdm	Network DDE DSDM	Manual	Disabled
NtLmSsp	NTLM Security Support Provider	Manual	Disabled
SysmonLog	Performance Logs and Alerts	Manual	Manual
PlugPLay	Plug and Play	Automatic	Automatic
Spooler	Print Spooler	Automatic	Enabled only in the File and Print role
ProtectedStorage	Protected Storage	Automatic	Automatic
RSVP	QoS Admission Control (RSVP)	Manual	Disabled
RasAuto	Remote Access Auto Connection Manager	Manual	Disabled
RasMan	Remote Access Connection Manager	Manual	Disabled
RpcSs	Remote Procedure Call (RPC)	Automatic	Automatic
Rpclocator	Remote Procedure Call (RPC) Locator	Manual	Enabled only in the DC role
RemoteRegistry	Remote Registry Service	Automatic	Automatic
NtmsSvc	Removable Storage	Automatic	Disabled
RemoteAccess	Routing and Remote Access	Disabled	Disabled
Seclogon	RunAs Service	Automatic	Disabled
SamSs	Security Accounts Manager	Automatic	Automatic
Lanmanserver	Server	Automatic	Automatic
SMTPSVC	Simple Mail Transport Protocol (SMTP)	Automatic	Disabled
ScardSvr	Smart Card	Manual	Disabled
ScardDrv	Smart Card Helper	Manual	Disabled
SENS	System Event	Automatic	Automatic

	Notification		
Schedule	Task Scheduler	Automatic	Disabled
LmHosts	TCP/IP NetBIOS Helper Service	Automatic	Automatic
TapiSrv	Telephony	Manual	Disabled
TlntSvr	Telnet	Manual	Disabled
TermService	Terminal Services	Disabled	Disabled
UPS	Uninterruptible Power Supply	Manual	Disabled
UtilMan	Utility Manager	Manual	Disabled
MSIServer	Windows Installer	Manual	Disabled
WinMgmt	Windows Management Instrumentation	Manual	Disabled
WMI	Windows Management Instrumentation Driver Extensions	Manual	Manual
W32Time	Windows Time	Automatic*	Automatic
LanmanWorkstation	WorkStation	Automatic	Automatic
W3svc	World Wide Web Publishing Service	Automatic	Enabled only in the IIS role
* - Automatic for a server in the domain. Manual if server belongs to a workgroup.			

Figure 3 - SampleHighSecurityPolicy.inf

```
[Version]
signature="$CHICAGO$"
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 90
MinimumPasswordLength = 7
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 30
LockoutDuration = 30
RequireLogonToChangePassword = 1
ForceLogoffWhenHourExpire = 1
[System Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 0
```

```
RestrictGuestAccess = 1
[Event Audit]
AuditSystemEvents = 2
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 2
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 2
CrashOnAuditFull = 0
[Registry Values]
machine\system\currentcontrolset\services\rdr\parameters\requiresecuritysignature=4,0
machine\system\currentcontrolset\services\rdr\parameters\enablesecuritysignature=4,0
machine\system\currentcontrolset\services\rdr\parameters\enableplaintextpassword=4,0
machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel=4,0
machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel=4,0
machine\system\currentcontrolset\services\netlogon\parameters\requiresignorseal=4,0
machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature
machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature=
machine\system\currentcontrolset\services\lanmanserver\parameters\enableforcedlogoff=4,0
machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect=4,0
machine\system\currentcontrolset\control\session manager\ protectionmode=4,1
machine\system\currentcontrolset\control\session manager\memory
management\clearpagefileatshutdown=4,0
machine\system\currentcontrolset\control\print\providers\lanman print
services\addprintdrivers=4,1
machine\system\currentcontrolset\control\lsa\submitcontrol=4,0
machine\system\currentcontrolset\control\lsa\restrictanonymous=4,1
machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel=4,0
machine\system\currentcontrolset\control\lsa\crashonauditfail=4,0
machine\system\currentcontrolset\control\lsa\auditbaseobjects=4,1
machine\software\microsoft\windows nt\currentversion\winlogon\shutdownwithoutlogon=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\legalnoticetext=1,This is a
where to put the legal mumbojumbo.
machine\software\microsoft\windows
nt\currentversion\winlogon\legalnoticecaption=1,WARNING! FOR OFFICIAL USE ONLY!!!!!
machine\software\microsoft\windows
nt\currentversion\winlogon\dontdisplaylastusername=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\cachedlogonscount=1,10
machine\software\microsoft\windows nt\currentversion\winlogon\allocatefloppies=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\allocatecdroms=1,1
[Privilege Rights]
seassignprimarytokenprivilege =
seauditprivilege =
sebackupprivilege = Backup Operators,Administrators
sechangenotifyprivilege = Authenticated Users
secreatepagefileprivilege = Administrators
secreatepermanentprivilege =
secreatetokenprivilege =
sedebugprivilege = Administrators
```

seincreasebaseprioritytprivilege = Administrators
seincreasequotaprivilege = Administrators
seloaddriverprivilege = Administrators
selockmemoryprivilege =
senetworklogonright = Authenticated Users,Users,Print Operators,Server Operators,Backup Operators,Administrators,Account Operators
seprofilesingleprocessprivilege = Administrators
seremoteshutdownprivilege = Administrators
serestoreprivilege = Backup Operators,Administrators
sesecurityprivilege = Administrators
seshutdownprivilege = Administrators
sesystemenvironmentprivilege = Administrators
sesystemprofileprivilege = Administrators
sesystemtimeprivilege = Administrators
setakeownershipprivilege = Administrators
[Registry Keys]
1="classes_root", 2, "D:(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;CO)(A;CI;0x10000000;;;SY)(A;CI;0xc0010000;;;SO)"
2="classes_root\.hlp", 2, "D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
3="classes_root\helpfile", 2, "D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
4="machine\software", 2, "D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)(A;CI;0x10000000;;;CO)(A;CI;0xc0010000;;;SO)S:P(SA;CIOISAFA;0x000d0006;;;WD)"
5="machine\software\classes", 1, ""
6="machine\software\microsoft\netdde", 2, "D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
7="machine\software\microsoft\protected storage system provider", 1, ""
8="machine\software\microsoft\secure", 2, "D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;CO)(A;CI;0x10000000;;;SO)(A;CI;0x10000000;;;SY)"
9="machine\software\microsoft\windows nt\currentversion\aedebug", 2, "D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)(A;CI;0x10000000;;;CO)(A;CI;0xc0000000;;;SO)"
a="machine\software\microsoft\windows nt\currentversion\compatibility", 2, "D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)(A;CI;0x10000000;;;CO)(A;CI;0xc0000000;;;SO)"
b="machine\software\microsoft\windows nt\currentversion\drivers", 2, "D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)(A;CI;0x10000000;;;CO)(A;CI;0xc0000000;;;SO)"
c="machine\software\microsoft\windows nt\currentversion\drivers.desc", 2, "D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)(A;CI;0x10000000;;;CO)(A;CI;0xc0000000;;;SO)"
d="machine\software\microsoft\windows nt\currentversion\drivers32", 2, "D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
e="machine\software\microsoft\windows nt\currentversion\embedding", 2, "D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)(A;CI;0x10000000;;;CO)(A;CI;0xc0000000;;;SO)"
f="machine\software\microsoft\windows nt\currentversion\font drivers", 2, "D:P

(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)"
10="machine\software\microsoft\windows nt\currentversion\fontmapper", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)"
11="machine\software\microsoft\windows nt\currentversion\fonts", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)
(A;CI;0x10000000;;;CO)(A;CI;0xc0000000;;;SO)"
12="machine\software\microsoft\windows nt\currentversion\fontsubstitutes", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)
(A;CI;0x10000000;;;CO)(A;CI;0xc0000000;;;SO)"
13="machine\software\microsoft\windows nt\currentversion\gre_initialize", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)
(A;CI;0x10000000;;;CO)(A;CI;0xc0000000;;;SO)"
14="machine\software\microsoft\windows nt\currentversion\image file execution options", 2,
"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
15="machine\software\microsoft\windows nt\currentversion\inifilemapping", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
16="machine\software\microsoft\windows nt\currentversion\mci", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)
(A;CI;0x10000000;;;CO)(A;CI;0xc0000000;;;SO)"
17="machine\software\microsoft\windows nt\currentversion\mci extensions", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)
(A;CI;0x10000000;;;CO)(A;CI;0xc0000000;;;SO)"
18="machine\software\microsoft\windows nt\currentversion\midimap", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)
(A;CI;0x10000000;;;CO)(A;CI;0xc0000000;;;SO)"
19="machine\software\microsoft\windows nt\currentversion\perflib", 2, "D:P
(A;CI;0x80000000;;;IU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
1a="machine\software\microsoft\windows nt\currentversion\perflib\009", 1, ""
1b="machine\software\microsoft\windows nt\currentversion\ports", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)
(A;CI;0x10000000;;;CO)(A;CI;0xc0000000;;;SO)"
1c="machine\software\microsoft\windows nt\currentversion\profilelist", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)
(A;CI;0x10000000;;;CO)(A;CI;0xc0000000;;;SO)"
1d="machine\software\microsoft\windows nt\currentversion\time zones", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
1e="machine\software\microsoft\windows nt\currentversion\type 1 installer\type 1 fonts", 2,
"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)
(A;CI;0x10000000;;;CO)(A;CI;0xc0000000;;;SO)"
1f="machine\software\microsoft\windows nt\currentversion\windows", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
20="machine\software\microsoft\windows nt\currentversion\wow", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)
(A;CI;0x10000000;;;CO)(A;CI;0xc0000000;;;SO)"
21="machine\software\microsoft\windows\currentversion\app paths", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
22="machine\software\secure", 2, "D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)
(A;CI;0x10000000;;;SY)(A;CI;0x10000000;;;CO)(A;CI;0x10000000;;;SO)"
23="machine\system", 2, "D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)
(A;CI;0x10000000;;;SY)"

24="machine\system\clone", 1, ""
25="machine\system\controlset001", 1, ""
26="machine\system\controlset002", 1, ""
27="machine\system\controlset003", 1, ""
28="machine\system\controlset004", 1, ""
29="machine\system\controlset005", 1, ""
2a="machine\system\controlset006", 1, ""
2b="machine\system\controlset007", 1, ""
2c="machine\system\controlset008", 1, ""
2d="machine\system\controlset009", 1, ""
2e="machine\system\controlset010", 1, ""
2f="machine\system\currentcontrolset\control", 2, "D:(A;CI;0x10000000;;;CO)
(A;CI;0xc0010000;;;SO)"
30="machine\system\currentcontrolset\control\graphicsdrivers", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
31="machine\system\currentcontrolset\control\lsa", 2, "D:P(A;CI;0x80000000;;;AU)
(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
32="machine\system\currentcontrolset\control\prioritycontrol", 2, "D:P
(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
33="machine\system\currentcontrolset\control\productoptions", 1, ""
34="machine\system\currentcontrolset\control\securepipeservers\winreg", 2, "D:P
(A;CI;0x10000000;;;DA)(A;CI;0xc0000000;;;BO)"
35="machine\system\currentcontrolset\control\session manager\executive", 2, "D:P
(A;CI;0x10000000;;;CO)(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)
(A;CI;0x10000000;;;SY)(A;CI;0xc0000000;;;SO)"
36="machine\system\currentcontrolset\control\session manager\memory management", 2,
"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
37="machine\system\currentcontrolset\control\timezoneinformation", 2, "D:P
(A;CI;0x10000000;;;CO)(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)
(A;CI;0x10000000;;;SY)(A;CI;0xc0000000;;;SO)"
38="machine\system\currentcontrolset\control\windows", 2, "D:P(A;CI;0x80000000;;;AU)
(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)(A;CI;0xc0000000;;;SO)"
39="machine\system\currentcontrolset\enum", 2, "D:P(A;CI;0x80000000;;;AU)
(A;CI;0x10000000;;;SY)"
3a="machine\system\currentcontrolset\hardware profiles\0001\software", 2, "D:P
(A;CI;GA;;;CO)(A;CI;GRGWSD;;;AU)(A;CI;GA;;;DA)(A;CI;GA;;;SY)"
3b="machine\system\currentcontrolset\hardware profiles\0001
\system\currentcontrolset\control", 2, "D:(A;CI;0x10000000;;;CO)(A;CI;0xc0010000;;;SO)"
3c="machine\system\currentcontrolset\hardware profiles\0001
\system\currentcontrolset\enum", 2, "D:(A;CI;0x10000000;;;CO)(A;CI;0xc0010000;;;SO)"
3d="machine\system\currentcontrolset\hardware profiles\0001
\system\currentcontrolset\services", 2, "D:(A;CI;0x10000000;;;CO)(A;CI;0xc0010000;;;SO)"
3e="machine\system\currentcontrolset\hardware profiles\current", 1, ""
3f="machine\system\currentcontrolset\services", 2, "D:(A;CI;0x10000000;;;CO)
(A;CI;0xc0010000;;;SO)"
40="machine\system\currentcontrolset\services\eventlog", 2, "D:P(A;CI;0x80000000;;;AU)
(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
41="machine\system\currentcontrolset\services\wintrust", 2, "D:P(A;CI;0x80000000;;;AU)
(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
42="users\.default", 2, "D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)

(A;CI;0x10000000;;;SY)"
43="users\.default\software\microsoft\netdde", 2, "D:P(A;CI;0x10000000;;;DA)
(A;CI;0x10000000;;;SY)"
44="users\.default\software\microsoft\protected storage system provider", 1, ""
45="users\.default\software\microsoft\windows\currentversion\policies", 2, "D:
(A;CI;0x10000000;;;CO)(A;CI;0xc0010000;;;SO)"
[File Security]
1="c:\", 0, "D:(A;CIOI;0xa0000000;;;AU)(A;CIOI;0x10000000;;;DA)(A;CIOI;0x10000000;;;SY)
(A;CIOI;0x10000000;;;CO)(A;;0x40000000;;;SO)"
2="c:\autoexec.bat", 2, "D:P(A;;0x10000000;;;DA)(A;;0x10000000;;;SY)
(A;;0xa0000000;;;AU)(A;;0xe0010000;;;SO)S:P(SA;CIOISA;0x00000110;;;WD)
(SA;CIOISAFA;0x000d0046;;;WD)"
3="c:\boot.ini", 2, "D:P(A;;0x10000000;;;DA)(A;;0x10000000;;;SY)(A;;0xe0010000;;;SO)S:P
(SA;CIOISA;0x00000110;;;WD)(SA;CIOISAFA;0x000d0046;;;WD)"
4="c:\config.sys", 2, "D:P(A;;0x10000000;;;DA)(A;;0x10000000;;;SY)(A;;0xa0000000;;;AU)
(A;;0xe0010000;;;SO)S:P(SA;CIOISA;0x00000110;;;WD)(SA;CIOISAFA;0x000d0046;;;WD)"
5="c:\inetpub", 1, ""
6="c:\ntbootdd.sys", 2, "D:P(A;;0x10000000;;;DA)(A;;0x10000000;;;SY)
(A;;0xe0010000;;;SO)S:P(SA;CIOISA;0x00000110;;;WD)(SA;CIOISAFA;0x000d0046;;;WD)"
7="c:\ntdetect.com", 2, "D:P(A;;0x10000000;;;DA)(A;;0x10000000;;;SY)
(A;;0xe0010000;;;SO)S:P(SA;CIOISA;0x00000110;;;WD)(SA;CIOISAFA;0x000d0046;;;WD)"
8="c:\ntldr", 2, "D:P(A;;0x10000000;;;DA)(A;;0x10000000;;;SY)(A;;0xe0010000;;;SO)S:P
(SA;CIOISA;0x00000110;;;WD)(SA;CIOISAFA;0x000d0046;;;WD)"
9="c:\pagefile.sys", 1, ""
a="c:\program files", 2, "D:P(A;CIOI;0x10000000;;;DA)(A;CIOI;0xa0000000;;;AU)
(A;CIOI;0x10000000;;;SY)(A;CIOI;0xe0010000;;;SO)"
b="c:\recycler", 1, ""
c="c:\temp", 2, "D:P(A;CIOI;0x10000000;;;CO)(A;;0xe0000000;;;AU)
(A;CIOI;0x10000000;;;DA)(A;CIOI;0x10000000;;;SY)"
d="c:\users", 1, ""
e="c:\winnt", 2, "D:P(A;CIOI;0xa0000000;;;AU)(A;CIOI;0x10000000;;;DA)
(A;CIOI;0x10000000;;;SY)(A;CIOI;0x10000000;;;CO)(A;CIOI;0xe0010000;;;SO)S:P
(SA;CIOISA;0x00000110;;;WD)(SA;CIOISAFA;0x000d0046;;;WD)"
f="c:\winnt\help", 2, "D:(A;;GW;;;AU)"
10="c:\winnt\profiles", 1, ""
11="c:\winnt\repair", 2, "D:P(A;CIOI;0x10000000;;;DA)(A;CIOI;0x10000000;;;SY)"
12="c:\winnt\system32\config", 2, "D:P(A;CI;0xa0000000;;;AU)(A;CIOI;0x10000000;;;DA)
(A;CIOI;0x10000000;;;SY)"
13="c:\winnt\system32\hpmon.dll", 2, "D:(A;;0xe0010000;;;PO)"
14="c:\winnt\system32\hpmon.hlp", 2, "D:(A;;0xe0010000;;;PO)"
15="c:\winnt\system32\localmon.dll", 2, "D:(A;;0xe0010000;;;PO)"
16="c:\winnt\system32\repl\export", 2, "D:(A;CIOI;0xe0010000;;;RP)S:P"
17="c:\winnt\system32\repl\import", 2, "D:(A;CIOI;0xe0010000;;;RP)S:P"
18="c:\winnt\system32\spool", 2, "D:(A;CIOI;0x10000000;;;PO)S:P"
19="c:\winnt\system32\spool\printers", 2, "D:P(A;CIOI;0x10000000;;;CO)
(A;CI;0xa0000000;;;AU)(A;CIOI;0x10000000;;;DA)(A;CIOI;0x10000000;;;PO)
(A;CIOI;0x10000000;;;SO)(A;CIOI;0x10000000;;;SY)"
1a="c:\~secure.nt", 1, ""

8. References

[1] Migliore, Matt. "Microsoft Says Security Emphasis is Paradigm Shift." Microsoft Certified Professional Magazine Online. November 2002. URL: http://mcpmag.com/news/article.asp?EditorialsID=528.

[2] Microsoft Corporation. "Windows NT 4.0 Server Baseline Security Checklist." Microsoft TechNet Website. 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/nt4svrcl.asp.

[3] Microsoft Corporation. "Windows 2000 Server Baseline Security Checklist." Microsoft TechNet Website. 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp.

[4] Microsoft Corporation. "Microsoft Security Bulletin MS02-064: Windows 2000 Default Permissions Could Allow Trojan Horse Program (Q327522)." Microsoft TechNet Website. 30 October 2002. URL: http://www.microsoft.com/technet/security/bulletin/MS02-064.asp

[5] Microsoft Corporation. "Default NTFS Permissions in Windows NT." Microsoft Support Services Website Knowledge Base Article Q148437. March 13, 1996. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q148437.

[6] Microsoft Corporation. "Default NTFS Permissions in Windows 2000." Microsoft Support Services Website Knowledge Base Article Q244600. October 26, 1999. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q244600.

[7] Microsoft Corporation. "To reapply default security settings." Microsoft TechNet Website. 2002. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/proddocs/SCM_revert.asp.

[8] Huie, Robert. "Security Configuration Tool and Template Settings Usefulness and Shortcomings of the Preconfigured Security Policy Templates that are Included with Windows 2000."SANS Institute's Information Security Reading Room Website. December 2000. URL: http://rr.sans.org/win/settings.php.

[9] Microsoft Corporation. "SP4 Security Configuration Manager Available for Download." Microsoft Support Services Knowledge Base Article Q195227. March 13, 1996. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q195227

[10] Microsoft Corporation. "Security Operations Guide for Windows 2000 Server." Microsoft TechNet Website. 2002. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/default.asp.