Global Information Assurance Certification Paper

Securing Microsoft's Windows 2000 Workstation with Security Templates

Steve Stern

Practical Assignment Version 3.1 (revised April 8, 2002)

Option 2 - Securing Windows 2000 with Security Templates

Table of Contents

TABLE OF FIGURES

Securing Microsoft Windows 2000

Introduction

With the wide spread use of Microsoft's Windows 2000 operating system, it becomes mandatory to explore some of the methods to tighten its security. Windows 2000 was built with security as a key component of the system, not an afterthought. However, Microsoft had to make a lot of difficult design choices when they developed the system. One design plan was to use a "sliding scale" (security vs. usability), the usability functions sometimes outweighed the security requirements. It is a very powerful operating system, scalable, stable and secure when set up correctly. Setup incorrectly however, and a Windows workstation is a target waiting to be attacked by hackers. This document explores some methods to tighten security using security templates. It is written with an emphasis on compliance with NASA's Procedures and Guidance for the Security of Information Technology, or NPG 2810 and is therefore a custom template. Although I will outline the procedures on how to create a security template, I did not write this template. An internal working group wrote it and is requesting that it be evaluated. The template will be evaluated as it was written with recommendations given at the end of this paper.

An outline of the paper is as follows:

- Introduce a security template that would be appropriate for the system
- Explain how the settings in the template would be applied to the system
- Apply the settings
- Test the system
- Evaluate the effectiveness of the template.
- Provide recommendations for improvement.

Description of system

The system being analyzed is a Windows 2000 workstation and used as a CAD (Computer Aided Drafting) under a NASA/government contract. Engineers and drafters use this workstation to produce electronic drawing files in support of International Space Station (ISS) and associated hardware. There are however some office automation functions that are performed on this workstation such as producing Word documents and reading email.

The hardware is:

- Intergraph ZX1 single CPU (600 MHz), 128 MB RAM
- Matrox graphics card w/ 8MB
- 18GB hard drive (SCSI)
- 21" monitor

The hard drive is to be setup with 2 partitions:

- C – Dynamic disk – 8GB
- D – Dynamic disk – 10GB

Additional software installed is

- Norton Antivirus 5.2
- Bentley MicroStation J (CAD Application)
- Bentley InterPlot 10 (Print/Plot application)
- Microsoft Systems Management Server (SMS) client software (automatic upon joining domain)
- Microsoft Office 2000 (Word, Excel, Outlook, etc…)

Windows 2000 Installation

Windows 2000 Server was installed from the Windows 2000 Server CDROM without a connection to any network. This was done in order to prevent any avoidable malicious attacks from infecting the machine while connected to the network.

All drives where formatted with NTFS in order to support Access Control Lists (ACL).

The system was installed at the default location, which is C:\WINNT. All other applications listed above were installed at this time and the drive was defragmented.

Post Windows 2000 Installation

Following the installation of the Windows 2000 operating system and the required applications, there are a few steps needed to bring the workstation up to the latest security level. This includes installing the latest Service Pack and any hot fixes.

Service Packs

Service packs are the means by which Windows 2000 product and security updates are distributed. Service packs are cumulative – that is to say that each new service pack contains all the fixes in previous service packs, as well as any new fixes. The latest Windows Service Pack can be obtained from:

http://www.microsoft.com/windows2000/downloads/servicepacks/default.asp

Service Pack 3 was installed and the workstation was rebooted. Following this, network connectivity was regained in order to finish installing any outstanding hot fixes.

Hot Fixes & Patches

There are a couple of tools provided by Microsoft to helps solve many of the problems associated with determining what hot fixes are needed. One popular method is to use Hfnetchk. Hfnetchk is a command-line tool that administrators can use to centrally assess

a computer or group of computers for the absence of security patches. Hfnetchk determines if a specific patch is installed on a given computer by evaluating and verifying three items: [1]

- The registry key that is installed by the patch
- The file version
- The checksum for each file that is installed by the patch.

Hfnetchk can be downloaded from:

support.microsoft.com/support/ kb/articles/q303/2/15.asp

To use NFNETCHK type (in a command prompt):

hfnetchk -v -z -s 1

The switches tell Hfnetchk to do the scan with the following changes:

- Output verbose or detailed mode (-v)
- Do not do registry check that hot fix key exists. Only check file details. (-z)
- Do not display note messages (notes are messages and can not be fixed by just the installation of a patch) (-s 1)

Hfnetchk Scan

After the installation, an Hfnetchk was run to ascertain the status of any outstanding security updates.

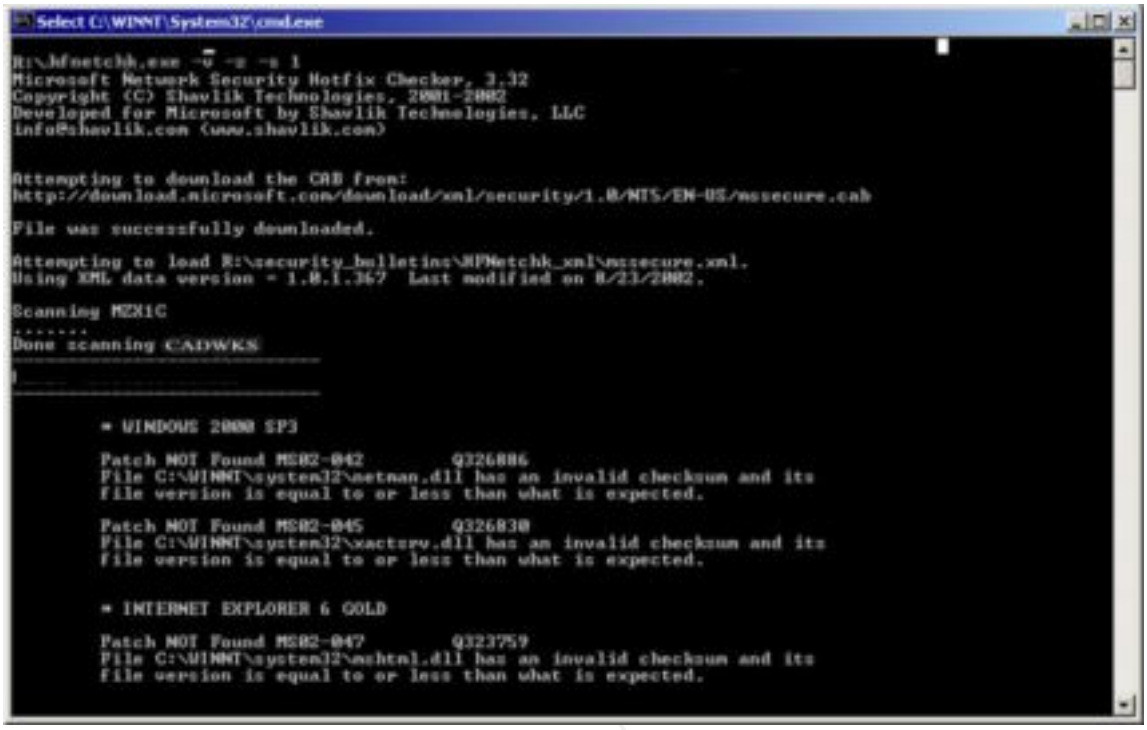

Figure 1 Hfnetchk Scan

All outstanding hotfixes were installed and the machine rebooted for the updates to take effect.

Norton Antivirus

Norton Antivirus virus definitions were updated and LiveUpdate was setup to update once a week to the Norton website. A virus scan was done on the machine.

At this point the patches and hot fixes have been downloaded and installed. The workstation was joined to a Active Directory domain and put into a test Organizational Unit (OU)

Description of the Template

Security Requirements of NPG 2810[2]

This workstation is a member of the NASA domain, and is connected to the Internet via a firewall. Therefore, it is required that safeguards and protection of the workstation and it's data be maintained under NASA Procedures and Guidance for the Security of Information Technology (NPG 2810). NPG 2810 applies to all NASA employees and NASA contracts as well as to Agency personnel and resources in deployment at non-Agency sites including colleges, universities, and other research establishments.

NPG 2810 describes that the NASA IT Security Program is to provide direction designed to ensure that safeguards for the protection of the integrity, availability, and confidentiality of IT resources (e.g., data, information, applications, and systems) are integrated into programs to support the missions of NASA.

The three components of IT resources that require protection are as follows:

a. **Integrity--**The ability to ensure that information, the applications processing that information, the information technology systems used to run that information, and the hardware configuration, connectivity, and the status of privilege settings cannot be altered during processing, storage or transmission.
b. **Availability--**The ability to ensure that data, applications, and systems are accessible when and where needed.
c. **Confidentiality--**The ability to ensure that information is disclosed only to those who have a valid need to possess it.

NPG 2810 is a document that was created by the security officers at each NASA facility, and ratified by the Chief Information Officers in the Agency. Simply stated, this is the authoritative reference for NASA on systems and information security. NPG 2810 was created to give the Agency as a whole, some overall guidance on how to integrate IT security into its standard business practices. Recently ratified, this document details the roles, responsibilities, and all requirements expected of NASA systems and personnel with respect to security. It provides direction so as to ensure that "safeguards for the protection of the integrity, availability, and confidentiality of IT resources are integrated into and support the missions of NASA." In addition to this, NPG 2810 defines security metrics and ways of gathering data about security incidents.

NPG 2810 states that:

- Protective controls need to be factored into all decisions concerning information technology resources.
- Security should not be an afterthought.
- A secure computing environment is based on managing risks to an appropriate level.
- Everyone is responsible for helping to ensure that computing resources are not exposed to undue levels of risk.
- All of NASA's information is considered valuable and sensitive to some degree.

The guidelines are what makeup the cornerstone of the Agency's information technology security philosophy.

A key factor in NPG 2810 is that security planning should be done throughout the lifecycle of a project or a mission. This includes doing a full risk assessment in the planning phases of a project. It also specifies that each project needs to have a security plan, which would include a "rules of proper use" by which each employee would abide.

NPG 2810 can be found at:

http://nodis3.gsfc.nasa.gov/library/displayDir.cfm?Internal_ID=N_PG_2810_0001_&page_name=main&search_term=%202810

NPG 2810 requires that systems adhere to a minimum standard known as a baseline. The baseline requirements are sets of technical, procedural, and physical IT security measures intended to ensure a reasonable level of security for a system. They are derived from "best practices" used by industry and the Government and are used in security planning as a benchmark for identifying risks to which a system may be exposed. The degree of compliance with these requirements is indicated in the IT Security Plan for the system. Typically the baseline requirements vary, depending on the information category of the system. The information categories, their abbreviations, and descriptions are as follows:

- **Mission Information (MSN)** --If the information, software applications, or computer systems in this category are altered, destroyed, or unavailable, the impact on NASA could be catastrophic.
- **Business and Restricted Technology Information (BRT)** --This category consists of information that NASA is required by law to protect. In general, if information in this category should be disclosed inappropriately, the disclosure could result in damage to employees, loss of business for NASA's partners and customers, contract award protests, or the illegal export of technology.
- **Scientific, Engineering, and Research Information (SER)** --All official NASA information held by NASA employees may be released publicly only in accordance with NASA regulations; however, systems in this category do not contain information for which the release is otherwise governed by law.
- **Administrative Information (ADM)** --This category includes systems, applications, and information that support NASA's daily activities, such as electronic mail, forms processing, networking, and management reporting.
- **Public Access Information (PUB)** --This category contains information, software applications, or computer systems specifically intended for public use or disclosure, such as a public Web site or hands-on demonstrations. The loss, alteration, or unavailability of data in this category would have little direct impact on NASA's missions, but it might expose the Agency to embarrassment, loss of credibility, or public ridicule.

The level of security needed on this workstation is considered “Business and Restricted Technology Information” (BRT) since most of our NASA engineering drawings are considered export controlled by U.S. State Department.

Some settings were also added to fit the desktop needs as well such as lockdown and bandwidth settings as well as to increase the level of security. Therefore, not all of the template settings are required by NPG 2810.

Reason for Choosing Template

This template was chosen because of requirements for compliance to NPG 2810 for NASA contract I work on and some analysis needs to be done before implementation. An internal working group developed this template and was put out to a team to help test it. In this paper I will first test the template and then make recommendations afterwards.

Template Security Settings

The security requirements of NPG 2810 were compiled and the following settings are to be the Group Policies for the deployment of Windows 2000 on the workstation. [2,3]

Note

Not all the settings will be discussed for the sake of overlooking some of the more critical settings. Also not all template settings are required by NPG 2810 and are added to improve functionality or security.

Account Policies

Password Policy

Password Length and Composition Requirements:

- Eight characters minimum and will contain at least one character each from at least three of the following sets of characters: uppercase letters, lowercase letters, numbers, and special characters.
- 90 days maximum
- Owner must have used a minimum of 10 passwords before reuse.
- Suspends, by system intervention, the user ID after five or fewer unsuccessful logon attempts or provides some form of system evasive action
- Notifies the System Administrator of user ID suspensions
- Number of days before user receives reminders to change password - 60 days maximum
- Number of days that user will be reminded to change password - 30 days maximum
- Number of days until user ID is suspended if user does not change password - 90 total days maximum
- Number of days until user ID is removed from the system - 180 total days maximum

The account lockout threshold was lowered to 3 in an effort to tighten security. The following template settings were added to comply with NPG 2810:

Policy Item	Setting	Notes
Enforce password history	10	Prevent users from rotating through their favorite passwords
Maximum password age	90	The period of time that a password is valid
Minimum password age	1	Prevent users from changing their passwords in an effort to get back to the previous password
Minimum password length	8	Help prevent passwords from being cracked
Passwords must meet complexity requirements	Enabled	Help prevent passwords from being cracked

Reversible encryption is not required so therefore is not enabled.

Lockout Policy

Policy Item	Setting	Notes
Account lockout threshold	3	Helps prevent brute force attacks
Account lockout duration	0	The setting of 0 indicates lockout until administrator unlocks
Reset account lockout counter after	30	This setting determines how long after a failed attempt the account lockout counter resets to 0.

Kerberos Policy

Policy Item	Setting	Notes
Enforce user logon restrictions	Enabled	The KDC validates every request for a session ticket by examining the user rights policy on the target computer to verify that the user has the right either to log on locally or to gain access to the computer from the network. It is also a check to ensure that the requesting account is still valid.
Maximum lifetime for service ticket	600 Min (10 Hrs)	"Service ticket" is a session ticket. Settings are in minutes. The setting must be more than ten minutes and less than the setting for "Maximum user ticket lifetime."
Maximum lifetime for user ticket	10 Hrs	A "user ticket" is a TGT and must be renewed after this time.
Maximum lifetime for user ticket renewal	7 Days	This is the maximum lifetime of a ticket (either a TGT or a session ticket, although the policy specifies that this is for a "user ticket"). No ticket can be renewed after this time.
Maximum tolerance for computer clock synchronization	5 min	The KDC server's clock and the Kerberos client's clock have to be synchronized to within a specified number of minutes. If the clocks are not synchronized within the specified number of minutes, tickets are not issued to the client. This is a deterrent in Replay attacks.

User Rights Assignment

Policy Item	Setting	Notes
Access this computer from the network	Authenticated Users	Everyone group is removed by this setting
Add workstations to domain	Domain Admins, Workstation Admins	Who can add a workstation to AD

Policy Item	Setting	Notes
Deny logon locally	Guest	Guest are specifically denied logon locally
Force shutdown from a remote system	Administrators, Domain Admins	Who can shutdown a machine remotely.
Generate security audits	System account, Administrators	Allows a process to make entries to the Security Log Managing Auditing and Security Log
Load and unload device drivers	Workstation Admins, Domain Admins	Install and remove device drivers.
Change System Time	Workstation Admins, Domain Admins	Prevent users from changing system time
Shut Down the System	Authenticated Users	Per A.6.1.5. System Shutdown/Restart

Per NPG 2810, the system should provide security safeguards to cover unscheduled system shutdowns (e.g., aborts) and subsequent restarts as well as for scheduled system shutdown and operational startup.

Security Options

Policy Item	Setting	Notes
Audit use of backup and restore privilege	Enabled	If Audit Privilege Use is enabled this security setting will enable the auditing of backup and restore user privileges.
Do not display last user name in logon screen	Enabled	Will present a blank username when doing CTRL+ALT+DEL
LAN Manager Authentication Level	Enabled (LM & NTLM - use NTLMv2 session security if negotiated)	Use NTLMv2 security if negotiated between machines. This is set for **interoperability** and not the highest setting which is Send NTLMv2 response only\refuse LM & NTLM
Message text for users attempting to log on	Enabled	"U.S. GOVERNMENT COMPUTER If not authorized to access this system, disconnect now. YOU SHOULD HAVE NO EXPECTATION OF PRIVACY By continuing, you consent to your keystrokes and data content being monitored."

Settings for Event Logs

NPG 2810 calls for journaling and monitoring of important system events. This is accomplished by event logs in Windows 2000 are used as an audit trail to investigate system or security problems. A process that accomplishes the following will be used:

- Ensures system journals record security-related events
- Records successful and failed logons/logoffs

- Records all successful and failed file opens and closes at the discretion of the line manager
- Records critical system file modification events or attempts
- Ensures journals identify programs being executed, users, source devices, files, and the time, date, and success or failure of all access attempts
- Logs and documents all aborts and restarts
- Provides audit trails or a journal of security-relevant events
- Reviews journals weekly or more frequently when problems are suspected
- Retains journals for at least 6 months

The following policy settings will meet the requirements of NPG 2810.

Local Policies

Audit Policy:

Policy Item	Success	Failure	Notes
Audit account logon events	Yes	Yes	This audit policy tracks login events with other computers from which the local computer was to authenticate the account.
Audit account management	Yes	Yes	Tracks changes to the security account database - when accounts are created, changed or deleted.
Audit directory service access	No	Yes	Tracks access failures to an Active Directory object.
Audit logon events	Yes	Yes	Tracks user logs on or off, or makes or cancels a network connection.
Audit object access	Yes	Yes	Tracks access to files, directories, registry keys, and printers
Audit policy change	Yes	Yes	Tracks changes to the security policy
Audit privilege use	Yes	Yes	Tracks when a user has exercised a privileged right, such as changing the system time
Audit process tracking	Yes	Yes	Tracks when a program or procedure has performed an action. This information is most useful to programmers who are tracking the details of program execution.
Audit system events	Yes	Yes	Tracks user restarts or shuts down his computer; or an event has occurred that affected the security of the operating system.

Event Log

Policy Item	Setting	Notes
Maximum application log size	20032K	Sets the maximum log size (file size)
Maximum security log size	20032K	Sets the maximum log size (file size)
Maximum system log size	20032K	Sets the maximum log size (file size)
Restrict guest access to application log	Enabled	Restricts the guest account from accessing the logs.
Restrict guest access to security log	Enabled	Restricts the guest account from accessing the logs.
Restrict guest access to system log	Enabled	Restricts the guest account from accessing the logs.

As stated in NPG 2810, event logs must reviewed weekly and retained for 6 months. This is not readily supported by Windows 2000 by default. Although I won't solve this issue here, I will make some recommendations to assist in further research and testing.

There are two tools that can be used to export event logs for consolidation:

- DUMPEVT from SomarSoft (http://somarsoft.com)
- Event Log Monitor from System Tools (http://www.systemtools.com)

However, since Windows 2000 does not have any way of backing up and storing Event Logs, and a manual method is not desired, a third part tool is needed. The tool must backup the event logs but allow easy access to them for later review. A quick search turned up a script that backs up and clears any Event Log that gets over 20 MB.

The script is as follows[4]:

```
strComputer = "."

Set objWMIService = GetObject("winmgmts:" _

   & "{impersonationLevel=impersonate, (Backup, Security)}!\\" _

      & strComputer & "\root\cimv2")

Set colLogFiles = objWMIService.ExecQuery _

   ("Select * from Win32_NTEventLogFile")

For each objLogfile in colLogFiles

   If objLogFile.FileSize > 20000 Then

      strBackupLog = objLogFile.BackupEventLog _

         ("c:\scripts\" & objLogFile.LogFileName & ".evt")

      objLogFile.ClearEventLog()

   End If

Next
```

Figure 2. Backup and Clear Large Event Logs Script Code

(Source: www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/logs/ScrLog05.asp)

The log would need to be backed up and could be viewed in the future. Another feature could be added to copy the logs to a database.
(Example:www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/logs/ScrLog07.asp)

As one can see, this requirement could get elaborate but can be accomplished.

File System Settings

NPG 2810 states that the system must be protected and restricted so that access to critical system files to a minimum number of authorized system support personnel.

The requirements of the file system and which Windows component fulfills the requirement are shown bellow:

NPG 2810 Requirement [2]	Windows Feature
Controls file access	NTFS ACL's
Identifies and protects critical system files.	Windows File Protection
Configuration control for critical system files	Windows File Protection

The template set the security levels on the %ProgramFiles% (C:\Program Files), %SystemDrive% (C:\), %SystemRoot% (C:\WINNT), and various files, executables, and directories within them in an effort to comply with NPG 2810.

The template has been adjusted to configure %SystemDrive% only. The setting is configured to replace existing permissions on all subfolders and files with inheritable permissions. The permissions are set for Full Control for Administrator and SYSTEM.

Settings are as follows:

File System Object	Default Power Use Permissions	Default User Permissions
c:\boot.ini	None	None
c:\ntdetect.com	None	None
c:\ntldr	None	None
c:\ntbootdd.sys	None	None
c:\autoexec.bat	None	RX
c:\config.sys	None	RX
\ProgramFiles	RX	RX
%windir%	RX	RX
%windir%*.*	RX	RX
%windir%\config*.*	RX	RX
%windir%\cursors*.*	RX	RX
%windir%\Temp	RX	Synchronize, Traverse, Add File, Add Subdir
%windir%\repair	RX	List

%windir%\addins	RX	RX
%windir%\Connection Wizard	RX	RX
%windir%\fonts*.*	RX	RX
%windir%\help*.*	RX	RX
%windir%\inf*.*	RX	RX
%windir%\java	RX	RX
%windir%\media*.*	RX	RX
%windir%\msagent	RX	RX
%windir%\security	RX	RX
%windir%\speech	RX	RX
%windir%\system*.*	RX	RX
%windir%\twain_32	RX	RX
%windir%\Web	RX	RX
%systemdir%	RX	RX
%systemdir%*.*	RX	RX
%systemdir%\config	List	List
%systemdir%\dhcp	RX	RX
%systemdir%\dllcache	None	None
%systemdir%\drivers	RX	RX
%systemdir%\CatRoot	RX	RX
%systemdir%\ias	RX	RX
%systemdir%\mui	RX	RX
%systemdir%\OS2*.*	RX	RX
%systemdir%\OS2\DLL*.*	RX	RX
%systemdir%\RAS*.*	RX	RX
%systemdir%\ShellExt	RX	RX
%systemdir%\Viewers*.*	RX	RX
%systemdir%\wbem	RX	RX
%systemdir%\wbem\mof	RX	RX

Move ACL Critical Files

It is recommended to move all access control list (ACL) critical files. Moving these files are important because hackers could use these tools to gain valuable information and launch rogue programs from the command line.

Place all commonly used administrative tools in a special directory out of %systemroot% and ACL them so that only administrators have full access to these files. For example create a directory called \CommonTools and place the following files in there:

xcopy.exe	wscript.exe	cscript.exe	net.exe	ftp.exe	telnet.exe
arp.exe	edlin.exe	ping.exe	route.exe	at.exe	finger.exe
posix.exe	rsh.exe	atsvc.exe	qbasic.exe	runonce.exe	syskey.exe

cacls.exe	ipconfig.exe	rcp.exe	secfixup.exe	nbtstat.exe	rdisk.exe
debug.exe	regedt32.exe	regedit.exe	edit.com	netstat.exe	tracert.exe
nslookup.exe	rexec.exe	cmd.exe			

System Services

Windows 2000 has services that can be configured for one of three settings: automatic, manual or disabled. It is recommended that services not required for proper operation of the system and it's applications be set to disabled. The services that are not needed will vary depending on the environment. This should be tested fully before wide scale implementation.

The following table lists those services that are disabled in this template:

Service	Startup	Comment
Alerter	Disabled	Send/receive messages to/from other machines
ClipBook	Disabled	Used to view contents of clipboard over the network
Computer Browser	Disabled	The more machines that run this service the more unreliable the Network Neighborhood gets. Can be a security risk - DoS attacks over the Internet target this service
DHCP Client	Disabled	All machines have a static IP address so not needed
FTP Publishing (if installed)	Disabled	Not needed, security risk
Indexing service	Disabled	Several exploits have been publicized where attackers viewed confidential information through service
Infrared Monitor service	Disabled	Possible way to attack systems, especially laptops
Internet Connection Sharing	Disabled	Not needed
NetMeeting Remote Desktop Sharing	Disabled	Not needed, security risk.
Simple Mail Transport Protocol	Disabled	Not needed, security risk. - DoS attacks over the Internet target this service
Simple TCP/IP services	Disabled	Provides seldom-used services from the UNIX world, such as Character Generator, Daytime, Discard, Echo, and Quote of the Day Can be a security risk - DoS attacks over the Internet target this service
Task Scheduler		Not needed
Telnet	Disabled	Not needed, security risk. Will use SSH if needed.

To set the template to disable these services, I used the Group Policy Object (GPO)[5] to set the startup mode and ACL for services by defining settings in *Computer Configuration, Windows Settings, Security Settings, System Services.* This is shown in figure 3.

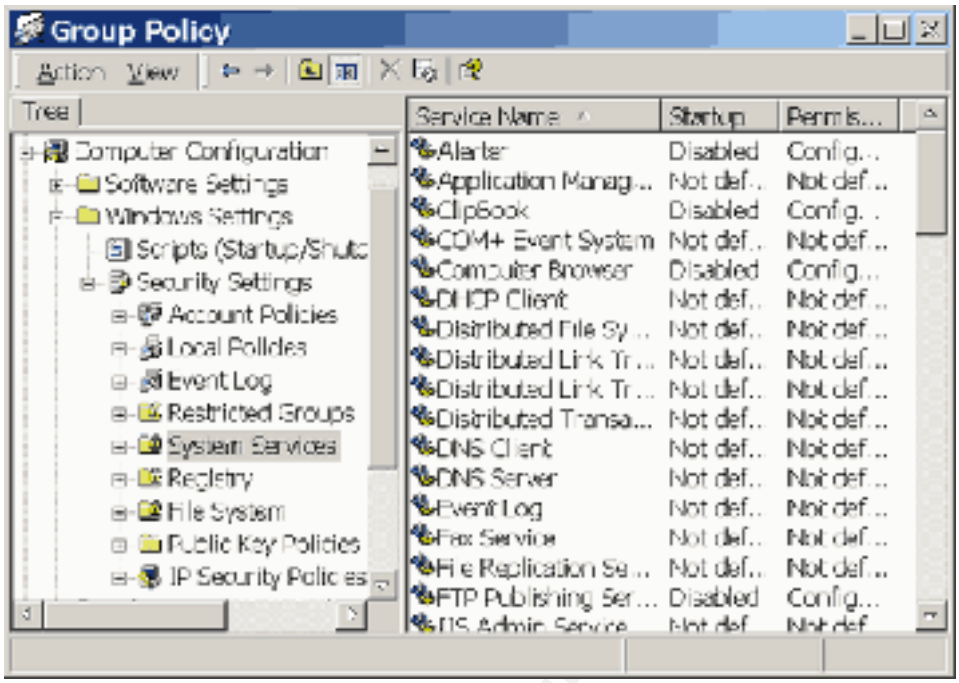

Figure 3. Setting System Services in the GPO MMC

A service's ACL specifies who can start, stop, and change the service. As with everything in Win2K, you can delegate authority over services to non-administrators. When you configure either the startup mode or the ACL of a service in Group Policy, you must configure the other as well. In other words, when you configure the startup mode of Alerter in a GPO, that GPO also modifies the service's ACL. This interaction is important because the default ACL on services in a GPO grants Full Control to Everyone for the service. If you disable a dangerous service but leave the ACL at its default, you are vulnerable to anyone who starts the service. Therefore, whenever you disable a potentially dangerous service in a GPO, you should also tighten control of the ACL by changing the default service ACL from granting everyone Full Control to granting Administrators and SYSTEM users with Full Control and granting Authenticated Users with Read access only. This can be done by selecting *Edit Security*… and setting the ACL accordingly. This is shown in figure 4.

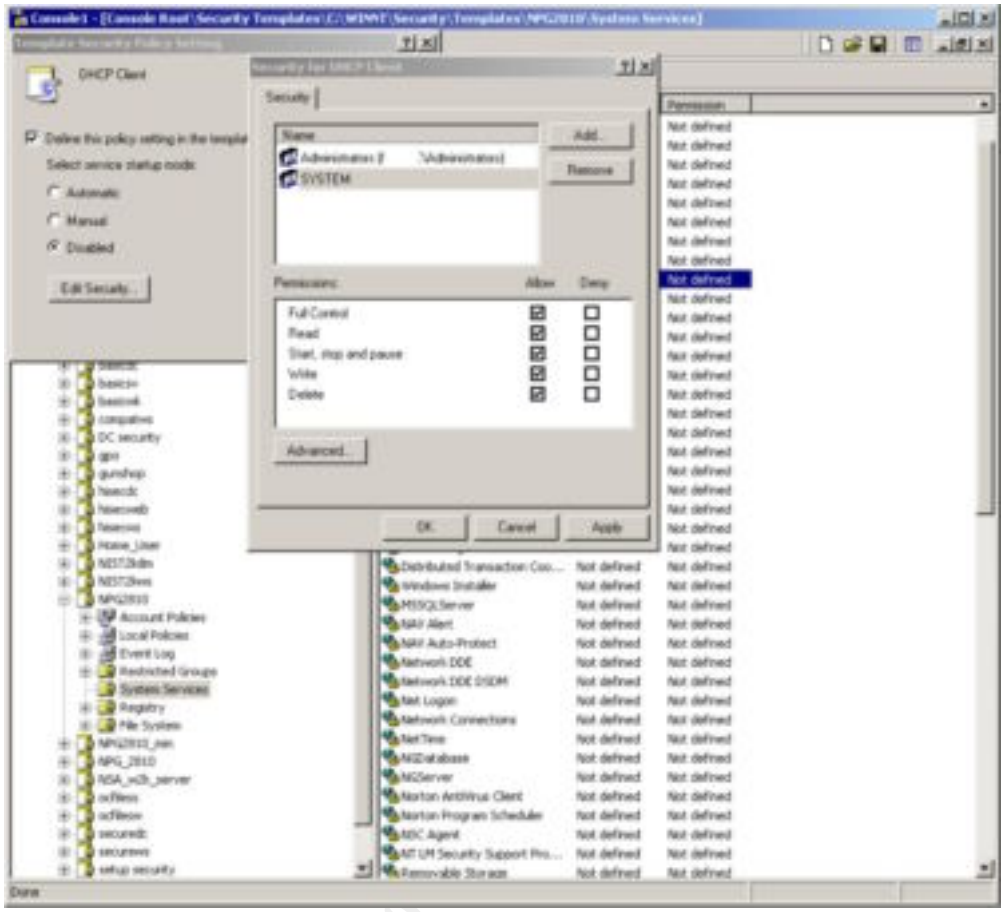

Figure 4. Setting ACL for Disabled Service in the GPO MMC

Registry Security Settings

The registry is the heart of a Windows 2000 and it is essential that one uses care when editing the registry.

The following registry settings should be considered for any security conscious environment. [6] As with any computer setting, testing is mandatory before wide scale deployment.

Restricting Information Available to Anonymous Logon Users

To restrict anonymous access to the registry and to prevent unauthenticated users from doing things like enumerating shares and local/domain users, the following registry setting is recommended (See Microsoft KB article Q143474):

Go to the following key in the registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

Create the following value:

Value Name: RestrictAnonymous
Data Type: REG_DWORD
Value: 1

Remove the OS/2 and POSIX Subsystems

If you are not using the OS/2 or POSIX subsystems (and people rarely do), removing them may improve performance and also close a potential security risk.

To remove the OS/2 and POSIX subsystems [7]:

- Delete the **\winnt\system32\os2** directory and all of its subdirectories.
- Use the Registry Editor to remove the following registry entries:

Key:	HKEY_LOCAL_MACHINE\SOFTWARE
Subkey:	Microsoft\OS/2 Subsystem for NT
Entry:	delete all subkeys
Key:	HKEY_LOCAL_MACHINE\SYSTEM
Subkey:	CurrentControlSet\Control\Session Manager\Environment
Entry:	Os2LibPath
Value:	delete entry
Key:	HKEY_LOCAL_MACHINE\SYSTEM
Subkey:	CurrentControlSet\Control\Session Manager\SubSystems
Entry:	Optional
Values:	delete entry
Key:	HKEY_LOCAL_MACHINE\SYSTEM
Subkey:	CurrentControlSet\Control\Session Manager\SubSystems
Entry:	delete entries for OS2 and POSIX

Registry ACL's

The following registry ACL changes are made by the template in an effort to lock down the registry. The permissions are set to Full Control for Administrator and SYSTEM.

Registry Object	Default Power User Permissions	Default User Permissions
HKLM\Software	Read	Read
HKLM\SW\Classes\helpfile	Read	Read
HKLM\SW\Classes\.hlp	Read	Read

HKLM\SW\MS\Command Processor	Read	Read
HKLM\SW\MS\Cryptography	Read	Read
HKLM\SW\MS\Driver Signing	Read	Read
HKLM\SW\MS\EnterpriseCertificates	Read	Read
HKLM\SW\MS\Non-Driver Signing	Read	Read
HKLM\SW\MS\NetDDE	None	None
HKLM\SW\MS\Ole	Read	Read
HKLM\SW\MS\Rpc	Read	Read
HKLM\SW\MS\Secure	Read	Read
HKLM\SW\MS\SystemCertificates	Read	Read
HKLM\SW\MS\Windows\CV\RunOnce	Read	Read
HKLM\SW\MS\W NT\CV\DiskQuota	Read	Read
HKLM\SW\MS\W NT\CV\Drivers32	Read	Read
HKLM\SW\MS\W NT\CV\Font Drivers	Read	Read
HKLM\SW\MS\W NT\CV\FontMapper	Read	Read
HKLM\SW\MS\W NT\CV\Image File Execution Options	Read	Read
HKLM\SW\MS\W NT\CV\IniFileMapping	Read	Read
HKLM\SW\MS\W NT\CV\Perflib	Read (via Interactive)	Read (via Interactive
HKLM\SW\MS\W NT\CV\SecEdit	Read	Read
HKLM\SW\MS\W NT\CV\Time Zones	Read	Read
HKLM\SW\MS\W NT\CV\Windows	Read	Read
HKLM\SW\MS\W NT\CV\AsrCommands	Read	Read
HKLM\SW\MS\W NT\CV\Winlogon	Read	Read
HKLM\SW\MS\W NT\CV\Classes	Read	Read
HKLM\SW\MS\W NT\CV\Console	Read	Read
HKLM\SW\MS\W NT\CV\ProfileList	Read	Read
HKLM\SW\MS\W NT\CV\Svchost	Read	Read
HKLM\SW\Policies	Read	Read
HKLM\System	Read	Read
HKLM\SYSTEM\CCS\Control\SecurePipeServers\w nreg	None	None
HKLM\SYSTEM\CCS\Control\Session Manager\Executive	Read	Read
HKLM\SYSTEM\CCS\Control\TimeZoneInformation	Read	Read
HKLM\SYSTEM\CCS\Control\WMI\Security	None	None
HKLM\Hardware	Read (via Everyone)	Read (via Everyone)
HKLM\SAM	Read (via Everyone)	Read (via Everyone)
HKLM\Security	None	None

The settings are configured to replace existing permissions on all subkeys with inheritable permissions.

Application of Security Template

The GPO template is to be used in a domain environment and therefore is built and tested in a domain environment. A test Organizational Unit (OU) is implemented for workstations and the GPO template will be the only policy in use at this time.

Note: some information such as domain name is removed due to security.

Group Policy Object (GPO).

A GPO is a virtual storage location for domain computer policies.[8] Different policies can be placed into different GPO's, and GPO's can each be applied to selected users or computers. Replication of the policies occurs under the control of the Windows 2000 File Replication Service (FRS). A GPO can be associated with many AD containers, and each AD container can have multiple GPO's associated with it.

Win2K stores Group Policy information in two locations: the Group Policy Container (GPC) and the Group Policy Template (GPT). The GPC is the Active Directory object associated with the GPO. The GPC and GPT contain the GPO's version and status information. The GPT is a set of files residing in the \sysvol folder, which can be found on domain controllers. In the GPT is found information about administrative templates, security, scripts, and software installation.

Create the Template

One can either create a new policy from scratch or modify one of the built-in policies. I chose to modify an existing one included with Windows. To create this policy, I used the Security Templates MMC. This is shown in figure 5.

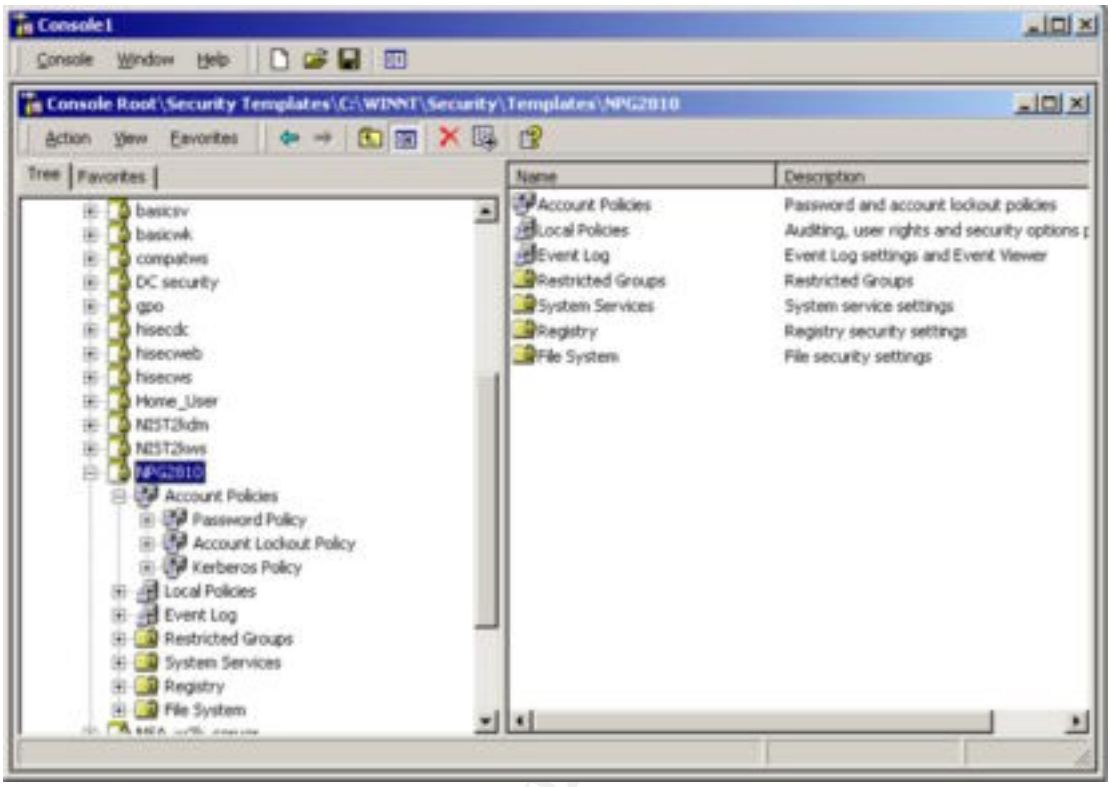

Figure 5 – Security Template MMC snap-in

I took the policy "hi*securews"* and renamed the template **NPG2810.** I then modified it to meet the settings required for NPG 2810 outline above. The template was saved to the default location of C:\WINNT\security\templates as NPG2810.inf. The template was then copied up to Domain Controller (DC) to the Netlogon share (%systemroot%\sysvol\DomainName\scripts).

Apply the template

After a template is created, the template settings can be imported into the GPO using Group Policy Editor (GPE). Using the Active Directory Users and Computers MMC snap-in does this. This tool is shown in figure 6

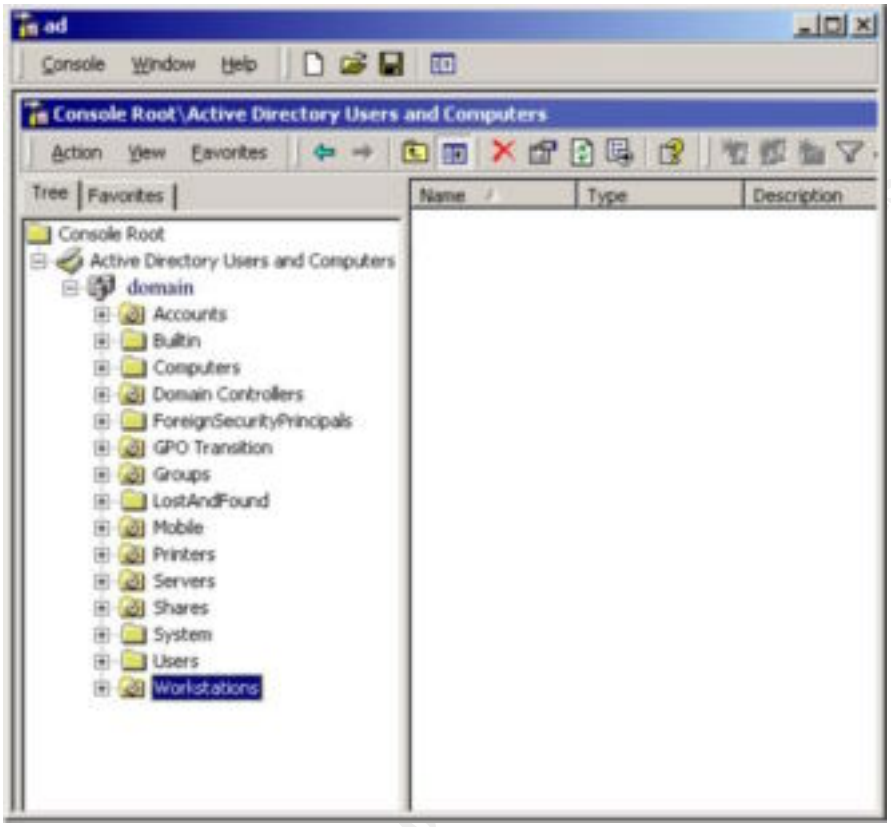

Figure 6 - Active Directory Users and Computers MMC snap-in

To make a template part of the group policy, select the group policy object Workstations in the Microsoft Management Console.

In this example the Policy is to be applied to the OU called Workstations by expanding the hierarchy, then right-clicking on the Active Directory container Workstations. Click Properties, and on the Group Policy tab, select New to create a new policy. Figure 8 shows the policy *CAD Test* created at the Workstation OU level.

Figure 7 – GPO CAD Test

By clicking on *Add…* the Group Policy dialog will appear. Next, navigate to Windows Settings|Security Settings. Now, right-click on Security Settings and select the Import Policy command from the resulting context menu shown in figure 8.

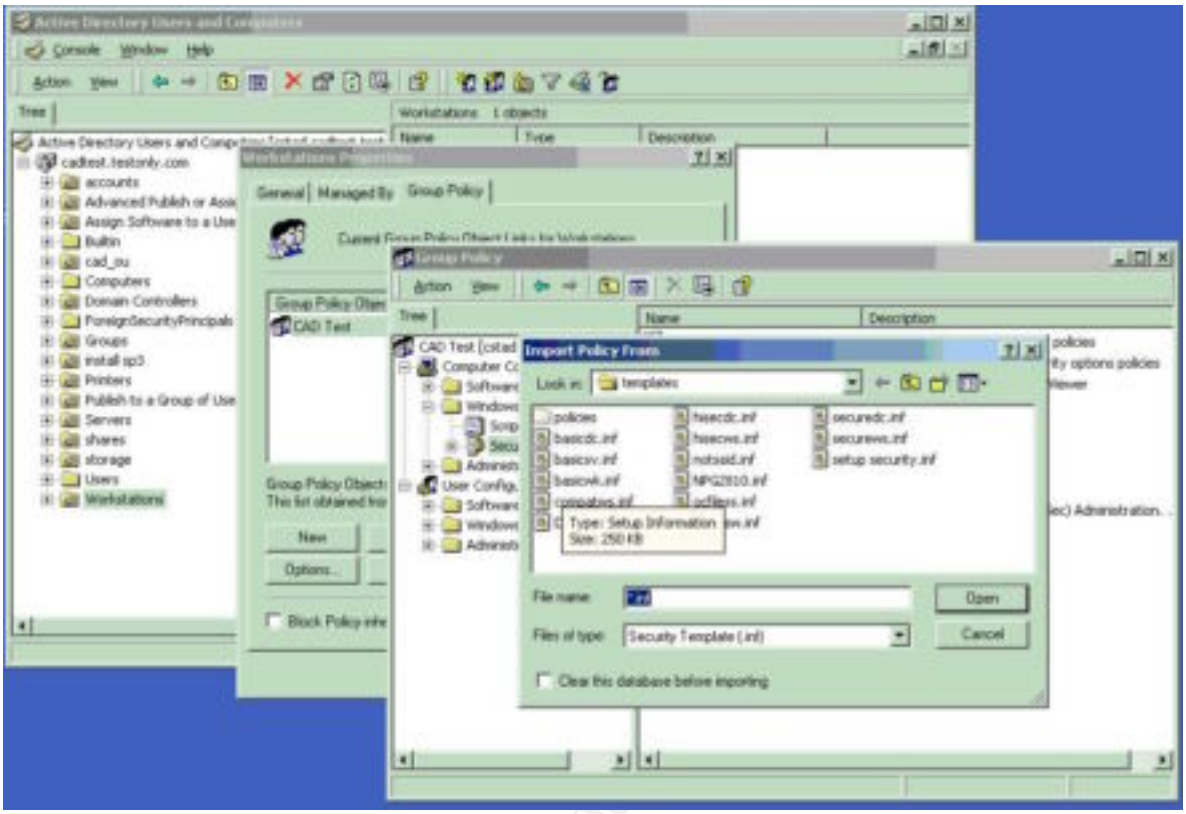

Figure 8 – Group Policy Importing

From the list of available security templates we select NPG 2810 and click OK.

This process applies all the settings configured in the template, to all the computers in the Workstations container but the process would apply to almost any container (e.g., site, domain, OU). This however does not apply to the Computers and Users containers. These are not organizational units; therefore, they cannot have Group Policy applied directly to them. Users or computers in these containers receive policies from GPOs scoped to the domain and site objects only. [9]

At this time the test workstation was added to the Workstation OU. The machine was rebooted for the GPO to take effect.

Keeping Up-to-date

Long-term Strategies for Group Policy Update

As Windows 2000 matures and the NASA domain changes, there will be a need to update the Group Policy from time-to-time. This can be done by adding other policies or refreshing the current Group Policy. The steps outlined above can be used to do this in the Active Directory Users and Computers MMC snap-in. In the container select Properties,

and on the Group Policy tab, select the appropriate button to get to the appropriate dialog to add, edit or delete a Group Policy.

Long-term Strategies for Hotfix and Patch Update

The Group Policy Team that delivered this template should review it often. The team should also meet with the various IT workgroups to get input into the effectiveness of the template and make changes as needed to keep pace with the security needs of the domain.

A major task of any Systems Administrator is keeping up with all of the Windows Service packs and hot fixes. The following are recommended sources of information for keeping up-to-date on patches and vulnerability information:

- Subscribe to the **Microsoft Security Notification Service** (www.microsoft.com/technet/security/bulletin/notify.asp). This is a free e-mail notification service that Microsoft uses to send information to subscribers about the security of Microsoft products.
- Download the **Windows Critical Update Notification 3.0 tool** (support.microsoft.com/default.aspx?scid=kb;en-us;Q224420&sd=tech) for notifications on when a Critical Update is released.
- Additionally, security patch and vulnerability information can be obtained at http://xforce.iss.net and www.ntbugtraq.com.

Keeping up on patches and vulnerability can be a daunting task and in a domain with thousands of machines it can be downright impossible. Hfnetchk is adequate on a standalone machine or a small workgroup but not really in a domain environment. To alleviate this problem, Microsoft has introduced a number of tools which are covered in the following section.

Microsoft Baseline Security Analyzer (MBSA)

MBSC is an installable tool that can scan the local machine or group of remote machines and report security violations and suggest a resolution. The advantage of MSBA is that more than just missing hot fixes are reported. It is recommended that the latest service pack be installed before running a MBSA scan to prevent extra, unnecessary steps. As far as workstations are concerned there are many valuable checks including:

Windows checks[10]

- Check for missing hotfixes and service packs
- Check for account password expiration
- Check for file system type on hard drives
- Check if autologon feature is enabled
- Check if the Guest account is enabled
- Check the RestrictAnonymous registry key settings

- Check the number of local Administrator accounts
- Check for blank and/or simple local user account passwords
- Check if unnecessary services are running
- List the shares present on the computer
- Check if auditing is enabled
- Check the Windows version running on the scanned computer

Desktop application checks

- List the Internet Explorer security zone settings per each local user
- List the Outlook security zone settings per each local user
- List the Office products security zone settings per each local user

There are however more checks made for servers, although they are not covered here.

This tools real value is in post installation testing which this paper will do during template evaluation.

Microsoft Baseline Security Analyzer can be obtained from:

www.microsoft.com/technet/security/ tools/Tools/mbsahome.asp

Some recommend using Windows Update (www.windowsupdate.microsoft.com) in which is a web based graphical interface. This may not be the best policy. According to Microsoft [11], the Microsoft Baseline Security Analyzer, which contains HFNETCHK.EXE, a hot-fix detecting program, contains different information than Windows Update and checks for more products. This is due to slight differences in update release policies and implementation across Microsoft. Microsoft is working toward improving the consistency and timeliness of updates and update notification released through these different mechanisms.

Also, new Windows Update content is released on a periodic, scheduled basis and so there may be a brief time before content that is available on other Microsoft Web sites becomes available on Windows Update

Software Update Services (SUS)

Microsoft recently introduced a new and free product named Software Update Services or SUS. SUS is designed to bring the functionality of the popular Windows Update site to the Corporate Network.

The basic premise of SUS is very similar to Windows Update[12]. SUS is composed of two components, the client and the server. The SUS client is installed on the workstation and configured to received Windows patches and updates from the domain SUS server(s). The SUS server is configured to retrieve Windows updates directly from Microsoft and store the updates locally. All of the content is digitally signed by Microsoft to

ensure the validity of the files. SUS will not accept any content that has not been signed by Microsoft or is incorrect, so this should hopefully ensure that the updates being distributed via SUS are accurate. After the updates are downloaded, the administrator has to validate the updates that have been downloaded so that they are ready to be distributed to the clients.

The advantages of using SUS are as follows[13]:

- Clients connect to one local source to retrieve any Windows updates as opposed to having all of the clients retrieve the update via the Internet.
- Administrators choose which updates need to be applied from the recommended patches allowing administrators to validate the updates before they are distributed to clients.
- It is free

As with any product there are disadvantages:

- It is in its first release
- SUS only supports Windows 2000 and XP critical updates and security rollups. No NT 4.0 or Win 9x support. Also no applications patches.
- Requirement of a client side installation.
- Present lack of notification of available updates on the SUS server that needs validation (planned feature for future update for SUS).
- Poor reporting on client update status. While the client updates are capable of writing system events and are also capable of updating a centralized IIS log file, there is presently no simple reporting method without combing through each client's system event log or parsing a cryptic IIS log file.

With security at Microsoft getting more attention these days, there should be more tools available than ever before. Which one is best depends on a lot of factors including price, ease of use and of course effectiveness.

Testing of Security Template

Test the template's security settings

After the NPG2810 Group Policy was applied, the workstation was tested in order to prove that there are no obvious anomalies that would hinder a user from doing common tasks and CAD work. Security settings were also tested to ensure that no unauthorized personnel could make changes to the system that would compromise reliability or security.

Password and Account Settings

An attempt was made to create a user with a 4-letter password. The following is the message returned:

Figure 9. Dialog warning of password policy violation

When a standard user tries to view the security log the following message appears:

Figure 10. Dialog warning that access to the security log is denied

When a standard user tries to change the system time, the following warning appears informing the user that it is not allowed:

Figure 11. Dialog warning that changing of system time is denied

So the password and account settings are functioning as designed, now we move on to application testing.

Test the system's functionality

Application Testing - MicroStation

MicroStation is a standard CAD application from Bentley Systems and is used primarily for engineering, civil and architectural drafting. It is very similar to AutoCAD in terms of system resources needed and disk space usage. MicroStation can do 3D modeling, however it uses a lot of system resources for rendering and even more for moving an object while it is rendered. In the test of this workstation a model of a Space Shuttle was brought up and rendered. This process consumed most (if not all) of the available system resources. This shows that the template does not introduce an unacceptable amount of overhead to the system.

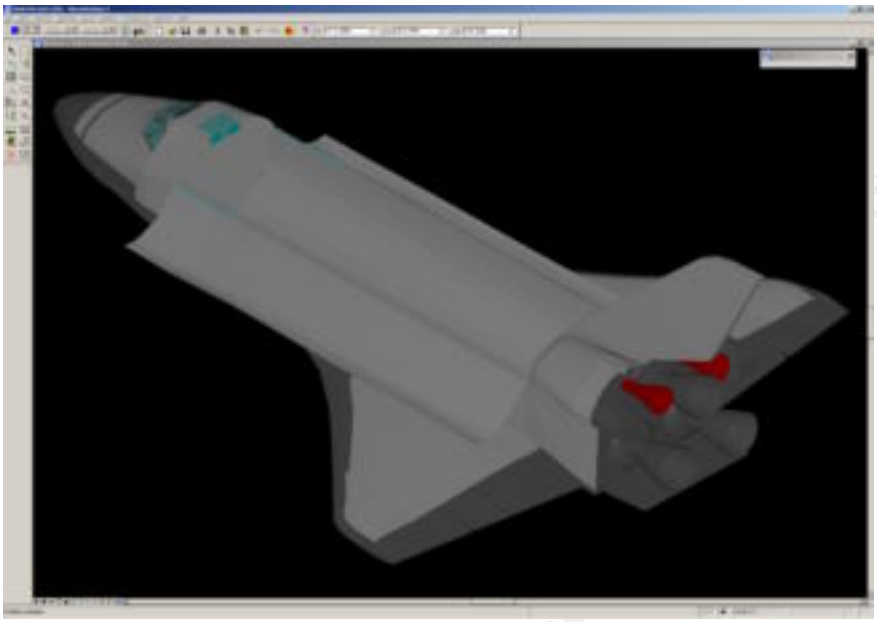

Figure 12. MicroStation Drawing of the Space Shuttle

Application Testing - MS Word

Microsoft Office 2000 was tested to ensure that office productivity tools would work and that security settings would not interfere with normal workload. A simple Word document was created and saved to the local hard drive. No anomalies were noticed.

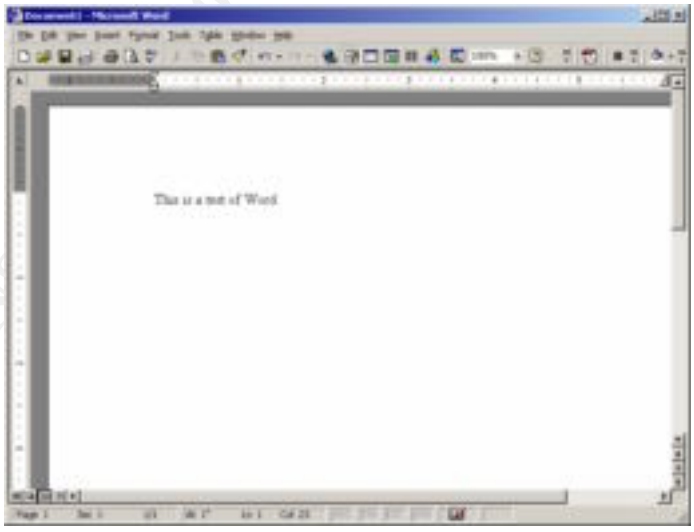

Figure 13. Microsoft Word in Action

Other applications open and work fine such as Excel and other MS Office 2000 application.

Application Testing - CD Burning with Nero

I decided to test the ability to burn a CD since a certain level of user permissions are required to do this. The Software used is Nero. It is burning to a SCSI HP CD ROM drive.

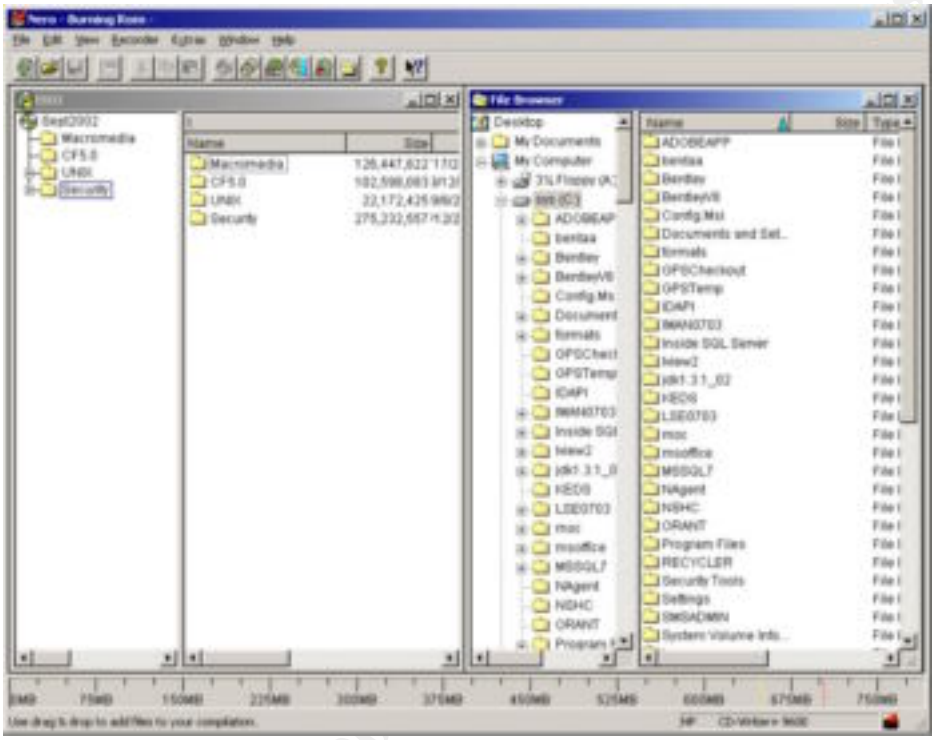

Figure 14. Nero CD-ROM Burner Image Creation

The CD was created (burned) without any errors.

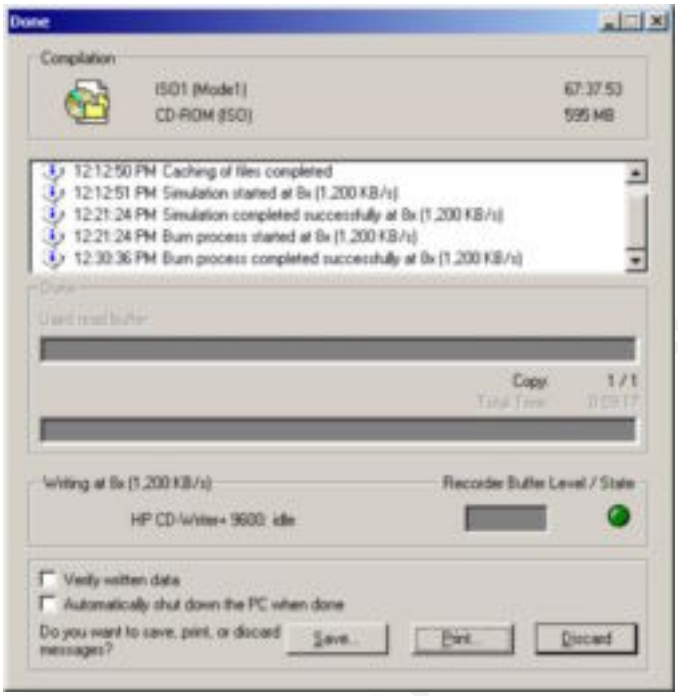

Figure 15. Nero CD-ROM Burner in Action

Evaluation of Security Template

Evaluate the template

This template seems fine for the environment the workstation is in. It meets (or exceeds) the requirements of NPG 2810 in many areas. Areas of positive results include:

- The account settings are quite adequate
- The event log settings are verbose enough for any administrator who wishes to know what is happening on a workstation and more than anyone could ever want to review
- The system service section disables some of the less commonly used and risky services
- The registry section secures the system registry to increase security
- The system files section secures system files to comply with NPG 2810

Potential Future Problem

I did notice one problem with Event Logs. Being that this workstation was put into a domain to be tested, the SMS (Microsoft Systems Management Server) account for the domain adds a lot of Security Log account access audit events.

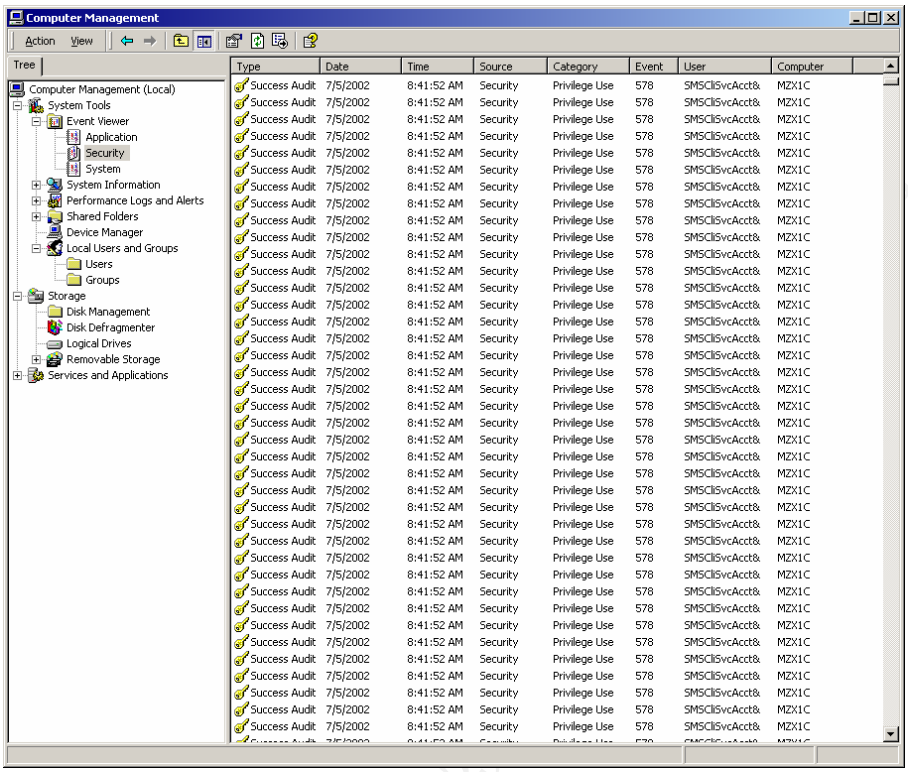

Figure 16. Security Event log

After 3 days of testing just on this workstation alone, the security log was 8 MB. Since the log size was set at a maximum of 20 MB, it is easy to imagine the log reaching its maximum after a week or so.

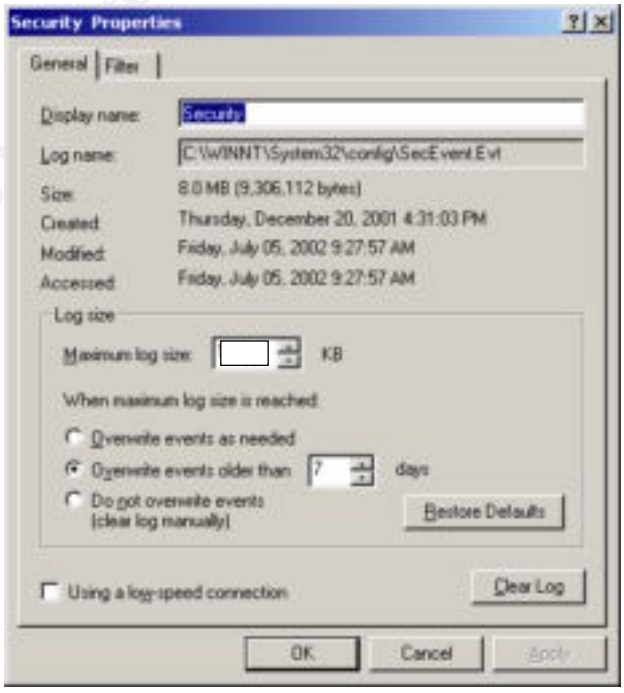

Figure 17. Security Event Log settings

Perhaps it would be prudent to either increase the log size settings in the policy to a value determined by further testing. I will defer this action because of the time needed to determine a proper solution for this problem and the fact that it did not cause a problem. It is just a noticed potential source of future problems.

Even though this is a short test, the workstation should work fine for this environment. Further testing over days is required before wide-scale deployment of this policy. No other anomalies were noted in this test and application testing is completed satisfactorily.

My recommendations are as follows:

- Test the Event Log size for an accurate expected size for the log files. If it is determined that each type of machine (workstation, server or DC) has vastly different log file sizes it may be determined that either they all get the maximum file size setting of each will need a different group policy.
- The group policy should be set so that the computer shuts down when the log files fills up. There is however, no requirement for this in NPG 2810.
- Rename the Guest and Administrator accounts. Perhaps even use a honey-pot Administrator account.

Other than this the template is satisfactory for this environment and meets the requirements for NPG 2810.

Again I should note that I did not author this template, I am simply evaluating it. It was done internally by a steering committee. Also it covers only the requirements of NPG 2810 to a particular workstation. It is not the final answer for all of the domains security needs. It is however a fine start.

Conclusion

Templates are a great feature and when used properly can greatly reduce the amount of time Systems Administrators spend visiting individual workstations. However, a complete understanding of what exactly the template is doing is mandatory. It is easy to see that one wrong setting can shutdown or cripple a company's computers. This can cost a company lost productivity time, embarrassment and/or compromise of security.

Proper testing is also mandatory especially before rolling one out in a large domain structure. This test involved only one type of machine, an Engineering workstation. Each type of machine should be tested including (but not limited to); file/application servers, standard PCs, web servers and domain controllers.

This template meets the requirements of NPG 2810. In the areas of account management, password aging and auditing it even exceeds the some of its requirements.

It can give management physical proof of adherence to the NASA policies for data security. I can therefore give management one less thing to worry about. It does not however solve all the domain's security vulnerabilities. A serious look at all aspects of a security defense needs to be looked at. After all, a chain is only as strong as its weakest link.

References

[1] Microsoft. "Microsoft Network Security Hotfix Checker (Hfnetchk.exe) (Q303215)", September 10, 2002. URL: http://support.microsoft.com/default.aspx?scid=KB;EN-US;q303215&

[2] NASA "NGP 2810.1" http://nodis3.gsfc.nasa.gov/library/displayDir.cfm?Internal_ID=N_PG_2810_0001_&page_name=main&search_term=%202810

[3] Judi Kling "Using Audit Policies to Secure Your Windows 2000 Network "http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnexnt00/html/ewn0054.asp

[4] Microsoft. "TechNet Script Center" September 18, 2002. URL: www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/logs/ScrLog05.asp

[5] Smith, Randy Franklin "Dangerous Services" January 4, 2001, Windows IT Security. URL: http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=16476

[6] Microsoft. "Group Policy Reference Table". September 18, 2002 URL: http://msdn.microsoft.com/library/en-us/gp/gpref.asp

[7] Labmice. "Windows 2000 Security Checklist". August 14, 2002. URL: www.labmice.net/articles/securingwin2000.htm

[8] WinNT Magazine. "Group Policy" September 18, 2002. URL: http://www.winntmag.com/articles/index.cfm?articleid=8144

[9] Microsoft. "Step-by-Step Guide to Understanding the Group Policy Feature Set". September 15, 2002. URL: www.microsoft.com/windows2000/techinfo/planning/management/groupsteps.asp

[10] Microsoft. "Microsoft Baseline Security Analyzer" September 15, 2002. URL: www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/mbsahome.asp

[11] Microsoft. "Windows Update FAQ". September 19, 2002, URL: www.microsoft.com/technet/itcommunity/Newsgroups/WUFAQ.asp?frame=true

[12] Microsoft. "Software Update Services" September 15, 2002. URL: www.microsoft.com/windows2000/windowsupdate/sus/

[13] Swynk . "Microsoft Software Update Services" September 15, 2002. URL: http://www.swynk.com/windows/rsmith/articles_13.asp

NPG2810.inf File Listing

```
[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 90
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 10
LockoutBadCount = 3
ResetLockoutCount = 30
LockoutDuration = -1
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 1
ClearTextPassword = 0
[System Log]
MaximumLogSize = 20032
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 20032
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 20032
RestrictGuestAccess = 1
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 3
AuditPrivilegeUse = 3
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 3
AuditDSAccess = 2
AuditAccountLogon = 3
[Kerberos Policy]
MaxTicketAge = 10
MaxRenewAge = 7
MaxServiceAge = 600
MaxClockSkew = 5
TicketValidateClient = 1
[Registry Values]
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownW
ithoutLogon=4,0
```

```
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ScRemoveOption=1,1
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,14
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\AllocateDASD=1,0
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SetCommand=4,0
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoti
ceText=1,"U.S. GOVERNMENT COMPUTERIf not authorized to access this system,
disconnect now. YOU SHOULD HAVE NO EXPECTATION OF PRIVACYBy continuing, you
consent to your keystrokes and data content being monitored."
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoti
ceCaption=1,WARNING
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDispl
ayLastUserName=4,1
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCA
D=4,0
MACHINE\Software\Microsoft\Non-Driver Signing\Policy=3,0
MACHINE\Software\Microsoft\Driver Signing\Policy=3,2
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrong
Key=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOr
Seal=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureCha
nnel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureCha
nnel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswo
rdChange=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\Enab
lePlainTextPassword=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\Requ
ireSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\Enab
leSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisco
nnect=4,15
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableFor
cedLogOff=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSe
curitySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSec
uritySignature=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown=4,1
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers=4,1
```

```
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,2
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,1
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects=4,0
[Privilege Rights]
SeMachineAccountPrivilege = Workstation Admins,Domain Admins
SeDenyInteractiveLogonRight = Guest
SeRemoteShutdownPrivilege = Workstation Admins,Domain Admins
SeAuditPrivilege = Workstation Admins,Domain Admins
SeLoadDriverPrivilege = Workstation Admins,Domain Admins
SeSystemtimePrivilege = Workstation Admins,Domain Admins
SeShutdownPrivilege = *S-1-5-11
SeNetworkLogonRight = *S-1-5-11
SeInteractiveLogonRight =
[Registry Keys]
"USERS\.DEFAULT\SOFTWARE\Microsoft\Protected Storage System
Provider",1,"D:AR"
"USERS\.DEFAULT\Software\Microsoft\NetDDE",2,"D:P(A;CI;GA;;;BA)(A;CI;GA;;;S
Y)(A;CI;GA;;;CO)"
"USERS\.DEFAULT",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;
;SY)(A;CI;GA;;;CO)"
"MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles",1,"D:AR"
"MACHINE\SYSTEM\CurrentControlSet\Enum",1,"D:AR"
"MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Services\EventLog",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers",2,"D:(A;CI;GR;;;W
D)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ProductOptions",2,"D:(A;CI;GR;;;W
D)"
"MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex",2,"D:(A;CI;GR;;;WD)
"
"MACHINE\SYSTEM\CurrentControlSet\Control\Computername",2,"D:(A;CI;GR;;;WD)
"
"MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Security",2,"D:P(A;CI;GR;;;BA
)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg",2,"D:P(
A;CI;GA;;;BA)(A;;GR;;;BO)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard
Layouts",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard
Layout",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SYSTEM\ControlSet010",1,"D:AR"
"MACHINE\SYSTEM\ControlSet009",1,"D:AR"
"MACHINE\SYSTEM\ControlSet008",1,"D:AR"
"MACHINE\SYSTEM\ControlSet007",1,"D:AR"
"MACHINE\SYSTEM\ControlSet006",1,"D:AR"
"MACHINE\SYSTEM\ControlSet005",1,"D:AR"
"MACHINE\SYSTEM\ControlSet004",1,"D:AR"
"MACHINE\SYSTEM\ControlSet003",1,"D:AR"
"MACHINE\SYSTEM\ControlSet002",1,"D:AR"
"MACHINE\SYSTEM\ControlSet001",1,"D:AR"
"MACHINE\SYSTEM\Clone",1,"D:AR"
"MACHINE\System",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;
;SY)(A;CI;GA;;;CO)"
```

```
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA
)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Windows",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)
(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time
Zones",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;
GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Svchost",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)
(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)
(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\SecEdit",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)
(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\ProfileList",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;
;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009",1,"D:AR"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Perflib",2,"D:P(A;CI;GR;;;IU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)
(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\IniFileMapping",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;G
A;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;C
I;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\FontMapper",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;
BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font
Drivers",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;C
I;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\EFS",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;C
I;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Drivers32",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;B
A)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Classes",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)
(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AsrCommands",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;
;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)(A;CI;SDGWGR;;;BO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AEDebug",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)
(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Accessibility",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA
;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion",2,"D:(A;CI;GR;;;WD)"
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies",1,"D:AR"
```

```
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer",1,"D:AR"
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy",1,"D:AR"
"MACHINE\SOFTWARE\Microsoft\SystemCertificates",2,"D:P(A;CI;GR;;;BU)(A;CI;G
R;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Secure",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI
;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider",1,"D:AR"
"MACHINE\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI
;GA;;;CO)"
"MACHINE\Software\Classes",2,"D:(A;CI;GR;;;WD)"
"MACHINE\Software",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA
;;;SY)(A;CI;GA;;;CO)"
[File Security]
"%SystemDirectory%\wbem\mof",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;O
ICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\wbem",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;
GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\ShellExt",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;O
ICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\mui",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;G
A;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\ias",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;
CO)"
"%SystemDirectory%\CatRoot",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OI
CI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\drivers",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OI
CI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\dllcache",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;
GA;;;CO)"
"%SystemDirectory%\dhcp",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;
GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\config",2,"D:P(A;CI;GXGR;;;BU)(A;CI;GXGR;;;PU)(A;OICI;GA
;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\spool\printers",1,"D:P(A;CI;GXGR;;;BU)(A;OICI;GXGR;;;PU)
(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\repl\export",1,"D:(A;OICI;SDGXGWGR;;;RE)"
"%SystemDirectory%\repl\import",1,"D:(A;OICI;SDGXGWGR;;;RE)"
"%SystemDirectory%\repl",1,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;
GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\ReinstallBackups",1,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;
;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\Setup",1,"D:AR"
"%SystemDirectory%\NTMSData",1,"D:AR"
"%SystemDirectory%\GroupPolicy",1,"D:AR"
"%SystemDirectory%\DTCLog",1,"D:AR"
"%SystemDirectory%\appmgmt",1,"D:AR"
"%SystemDirectory%",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;
BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)(A;OICI;GXGR;;;WD)"
"%SystemRoot%\Web",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;B
A)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemRoot%\twain_32",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;G
A;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemRoot%\speech",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;
;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemRoot%\security",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;G
A;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
```

```
"%SystemRoot%\msagent",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA
;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemRoot%\java",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;
BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemRoot%\Driver
Cache",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA
;;;SY)(A;OICI;GA;;;CO)"
"%SystemRoot%\Connection
Wizard",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;G
A;;;SY)(A;OICI;GA;;;CO)"
"%SystemRoot%\addins",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;
;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemRoot%\Temp",2,"D:P(A;CI;0x100026;;;BU)(A;CI;0x100026;;;PU)(A;OICI;G
A;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemRoot%\Tasks",1,"D:AR"
"%SystemRoot%\repair",2,"D:P(A;CI;GXGR;;;BU)(A;CI;GXGR;;;PU)(A;OICI;GA;;;BA
)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemRoot%\Registration",1,"D:AR"
"%SystemRoot%\Profiles",1,"D:AR"
"%SystemRoot%\Offline Pages",1,"D:AR"
"%SystemRoot%\debug",1,"D:AR"
"%SystemRoot%\CSC",1,"D:AR"
"%SystemRoot%\explorer.exe",2,"D:(A;;GXGR;;;WD)"
"%SystemRoot%",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A
;OICI;GA;;;SY)(A;OICI;GA;;;CO)(A;;GXGR;;;WD)"
"%ProgramFiles%",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)
(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"c:\config.sys",2,"D:P(A;;GXGR;;;BU)(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
"c:\autoexec.bat",2,"D:P(A;;GXGR;;;BU)(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY
)"
"c:\ntbootdd.sys",2,"D:P(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
"c:\ntldr",2,"D:P(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
"c:\ntdetect.com",2,"D:P(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
"c:\boot.ini",2,"D:P(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
[Version]
signature="$CHICAGO$"
Revision=1
[Profile Description]
Description=Security Template for NASA NPG 2810
[Service General Setting]
Alerter,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSD
RCWDWO;;;SY)"
ClipSrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSD
RCWDWO;;;SY)"
Browser,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;LA)(A;;CCDCLCSWRPWPDTLOCRSD
RCWDWO;;;SY)"
Dhcp,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;LA)(A;;CCDCLCSWRPWPDTLOCRSDRCW
DWO;;;SY)"
cisvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;LA)(A;;CCDCLCSWRPWPDTLOCRSDRC
WDWO;;;SY)"
SharedAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;LA)(A;;CCDCLCSWRPWPDTL
OCRSDRCWDWO;;;SY)"
mnmsrvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;LA)(A;;CCDCLCSWRPWPDTLOCRSD
RCWDWO;;;SY)"
Schedule,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;LA)(A;;CCDCLCSWRPWPDTLOCRS
DRCWDWO;;;SY)"
```

```
TlntSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;LA)(A;;CCDCLCSWRPWPDTLOCRSD
RCWDWO;;;SY)
```

Last Updated: July 26th, 2017

Upcoming Training

SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**