Global Information Assurance Certification Paper

Securing a Windows 2000 Application Server With Security Templates

Version 3.1

By Josh Sprenger

TABLE OF CONTENTS

SUMMARY

Windows 2000 contains an essential tool, Group Policy, which along with its subset of tools, eases the security administration across an enterprise. These tools provide a means of distributed security configuration across an environment. Windows NT contained a disparate set of tools used to configure different security settings. Often, changing a single security setting meant making the same change on every computer in the environment. Group Policy allows security configurations to be altered within a single set of tools, which can then be deployed across the enterprise.

Security Templates are text-based files that contain a wide variety of security settings that can be defined, altered, saved, and then applied through Group Policy. The settings that can be defined include Account Policies, Local Policies, Event Log, Restricted Groups, System Services, Registry, and File System. A number of organizations, including Microsoft, SANS, and NSA, provide pre-defined Security Templates to serve as recommended security configurations for different types of servers and workstations. These pre-defined templates provide an excellent baseline from which to start customizing for individual environments.

This Practical will focus on Security Templates and the process of selecting, testing, and analyzing a template for a specific enterprise. The first section will describe the company and its current systems environment, as well as identify the individual server type the selection will be based upon. The next sections will identify a Security Template to apply to the chosen system and then go into a detailed description of all security policies defined by the selected template. The following sections will explain how the template will be applied and test both the security settings of the template and the system's functionality with the template applied. The last section will analyze the template to identify the positives and the negatives associated with the template as applied to the individual system and the environment as a whole.

DESCRIPTION OF THE SYSTEM

Stinky Feet Shoes is an international shoe company that employs 15,000 people across its 10 plants in the US, five plants in Canada, and at its corporate offices in Stinkyville. Stinky Feet's corporate headquarters holds the company's data center where the company is undergoing a migration from Windows NT 4.0 to Windows 2000. Management expects significant improvements in security with the new OS and directory structure.

One of the major required areas of enhancement is in security, which is extremely lax under NT 4.0 environment. End-users currently have local Administrator privileges to their workstations in NT 4.0. Additionally, application owners and all support personnel have local Administrator rights on their NT 4.0 application servers. Many servers allow the Everyone group full access to directories holding vital application files and confidential data. Password policy and auditing are inadequate. Stinky Feet has learned its lesson the hard way with such ineffective security. Some of the issues Stinky Feet would like to see improved on include:

- The high number of help desk calls due to employees accessing administrative tools they do not entirely understand, resulting in configuration errors.
- Server downtime because of employees corrupting operating system files and the registry.
- Lack of emphasis on password policy allowing attackers to break into systems.
- Failure to lock down sensitive accounts.
- Lack of adequate audit policy.

Stinky Feet's management and the company's IT Security group are determined to institute a least privileged security model. Least privileged means "that a resource, or process, has no more privileges than necessary to be able to fulfill its functions." (Harris, p. 238) Therefore, the company will limit all resources using workstations and servers to access only what is necessary to complete their everyday tasks.

The focus of this research and analysis will be on Stinky Feet's Windows 2000 application server running the "StrongSuite Options" application. This application contains a proprietary database that keeps track of employee stock options. The application server is supported by a staff of three and is used by 35 members of the StinkyFeet Human Resource department. The application is client-server based, with the Human Resource users having a client-side application on their Windows 2000 Workstations. The application receives stock price updates every night through FTP from a mainframe.

Under the company's Windows 2000 security policy, security access to this server will follow a least privileged security model. While Administrator access to a server would be an easy fix for providing the support group the rights they require, it would clearly give them more rights than necessary and not adhere to the least privileged security model.

The support group will need to be able to log on to the server. The proprietary database on the server has database performance and maintenance tools available only on the server itself. The vendor of the software offers neither a client version of the tools to allow remote connections to the database, nor does the vendor provide a Microsoft Management Console snap-in for the tools. Company policy prevents application support groups from having local access to the computer console. The IT Security group has decided to resolve the issue by granting them Terminal Services access.

Additionally, the support group will require Read and Write access to the E:\Program Files\StrongSuite directory to complete database maintenance and cleanup. The group will need this access to read and delete log files as well. The support group will also require the ability to start and stop the StrongSuite Option and StrongSuite Database services.

Further rights will have to be granted to the Human Resources end-user group and the FTP account writing data from the mainframe. The only access the Human Resources end-user group will require to the server is read access to the E:\Program Files\StrongSuite\Reports directory to be able to access reports generated by the application. The FTP account will require write access to the E:\Program Files\StrongSuite\FTP directory.

Software Configuration

The software configuration of the server is detailed in the chart below.

Operating System	Microsoft Windows 2000 Advanced Server
Service Pack	Service Pack 3.0 and all critical security patches
Internet Browser	Internet Explorer 6.02
Anti-Virus	Norton Anti-Virus Corporate Edition 7.60

Hardware Configuration

The hardware configuration of the server is detailed in the chart below.

Base:	PowerEdge 2650, DUAL Intel XEON 2.4Ghz/512K Cache
Additional Processors:	DUAL Intel XEON 2.4Ghz
Memory:	2 GB DDR SDRAM
Keyboard:	Standard Windows Keyboard, Grey
1st Hard Drive:	36GB 10K RPM Ultra 320 SCSI Hard Drive
2nd Hard Drive:	36GB 10K RPM Ultra 320 SCSI Hard Drive
Primary Controller:	PERC3/Di 128MB (2 Internal Channels) - Embedded RAID
Floppy:	3.5 in, 1.44MB, Floppy Drive
Operating System:	Windows 2000 Advanced Server
Mouse:	Logitech Mouse, Grey
Network Adapters:	Dual Onboard 10/100/1000 Ethernet adapter
CD-ROM:	24X IDE CD-ROM

SELECTING A TEMPLATE

Stinky Feet's management is clearly looking to progress to a much more secure environment with its migration to Windows 2000. The least privileged security model requires that no unnecessary access be allowed. Selecting the right Security Template can lock down the server so much of the default server access, that is unnecessary for users and support groups to complete their tasks, is secured.

While Microsoft offers workstation, server, and domain templates aimed at high security, it does not offer a template as comprehensive as what the NSA offers. The NSA offers a Security Template, the W2K_Server template that offers security settings geared towards member servers. Additionally, the NSA's template offers higher security than even Microsoft's "hisecws" and "hisecdc" templates geared towards high security for workstations, servers, and domain controllers.

Comparing the NSA's W2K_Server template to Microsoft's "hisecdc" template, the W2K_Server has higher security in most areas. The W2K_Server template locks down sensitive operating system files and registry keys. The "hisecdc" template does not define any of these settings. The W2K_Server template defines many of the policies under "User Rights Assignment," while the "hisecdc" template leaves all these settings undefined. The only area the "hisecdc" issuance offers higher security is with certain settings within account lockout policy and within password settings. However, settings in these areas should have higher security on a Domain Controller, but would likely prove to sacrifice availability more than necessary on a server.

Measuring NSA's W2K_Server template security up to Microsoft's "hisecws" template, the W2K_Server once again offers improved security in most areas. The "hisecws" template does not define any of the system file settings or registry key settings. The W2K_Server template locks down sensitive operating system files and registry keys. The W2K_Server template defines many of the policies under "User Rights Assignment," while the "hisecws" template leaves all these settings undefined. The "hisecws" issuance offers higher security in the Restricted Groups area, restricting the Administrators group. However, the W2K_Server template offers high security in more areas.

SECURITY SETTINGS

ACCOUNT POLICIES

This area of the template deals with user account security. Although this area is defined within the template, it will not be effective for domain user accounts. Domain user account policy will be defined by the default domain policy, even if this policy is defined and placed within an OU or if it were configured with "No Override" or "Block Inheritance." A domain can have only one set of account policies and the domain controllers within the domain implement that policy. However, it is good practice to define these settings for when the template is used for local security policy so these settings will be effective for local user accounts.

Password Policy

This policy governs password history, minimum and maximum age, length, complexity requirements and whether to store the password with reversible encryption.

Policy	Computer Setting
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	12 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption for all users in...	Disabled

Enforce Password History This setting establishes the number of times a unique password must be used before an old password may be repeated. This can be set at a minimum of 0 and a maximum of 24. If this value is set to 0, the user may instantly regress to the password she was using before. In this case, the NSA has set Enforce Password History at the maximum of 24, so a user would have to go through 24 different passwords before reverting back to her original one. This setting is made more effective with Minimum Password Age, which can prevent users from continually changing their passwords until they are allowed to return to their original one (discussed further below).

Maximum Password Age This policy defines the longest amount of time that a user may have the same password before being required to change it. This value may be set at a minimum of 0 days and a maximum of 999 days. A value of 0 is would result in a password that never expires. The NSA has configured the Maximum Password Age setting to 90 days that will require users to change their password every 90 days.

Minimum Password Age This setting defines the least amount of time that a user must wait before changing her password. The minimum and default value is 0 days and the maximum is 998 days. A value of 0 would allow a user to change her password immediately. The NSA has set Minimum Password Age at one day that will prohibit users from changing their passwords for one day after they have created a new password.

Minimum Password Length This setting defines the minimum number of characters a password must be. Although Windows 2000 accepts passwords up to 127 characters in length, the maximum the Microsoft Security Template interface allows this to be set at is 14 characters. The minimum is one character. The NSA sets Minimum Password Length at 12 characters for this template, which would require users to create passwords that contain at least 12 characters.

Password Must Meet Complexity Requirement This setting defines whether a users password will have to meet Windows 2000's password complexity requirement. When this setting is enabled, it will require a user's password to include characters in three of the following four classes:

- Upper Case Letters
- Lower Case Letters
- Numbers
- Special Characters (i.e. ?, @, #, etc.)

Additionally, enabling complexity requirement will prevent users from using their log on names as a password. Once this setting is in place, it will only take effect once a user changes her password; existing passwords will not be affected. This template has this setting enabled.

Store Password Using Reversible Encryption This setting will store passwords using a two-way hash function when it is enabled. This is sometimes necessary for applications that require a user's password for authentication. The NSA has disabled this setting.

Account Lockout Policy

This policy includes the settings on account lockout duration, account lockout threshold and resets of the account lockout counter.

Policy	Computer Setting
Account lockout duration	15 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	15 minutes

Account Lockout Duration This setting determines the amount of time an account will remain locked out once it reaches the account lockout threshold. This can be set at a minimum of 0 to a maximum 99,999 minutes. When this is configured to be 0, the account will be locked out indefinitely until the administrator unlocks it. Here it is configured to be 15 minutes; consequently the user will be locked out for 15 minutes once she reaches the account lockout threshold.

Account Lockout Threshold This setting establishes the number of failed logon attempts a user is allowed before being locked out. This can range from a minimum of 0 attempts to a maximum of 999 logon attempts. A setting of 0 will result in accounts not locking out. The NSA has configured this setting at three resulting in users being locked out after three invalid attempts.

Reset Account Lockout Counter After This setting determines the amount of time before the failed logon counter is reset. This value can be a minimum of one minute to a maximum of 99,999 minutes. This template is configured with a setting of 30 minutes. With the Account Lockout Threshold set at five, a user would be able to have four failed logons, then waited 15 minutes, then be once again granted five invalid logon attempts before being locked out. However, once five failed logon attempts are reached within 15 minutes, the account would be locked out.

Kerberos

The Kerberos policy settings specify the configuration of Kerberos authentication including logon restrictions, lifetime for service and user tickets, and tolerance for computer clock synchronization. All settings for this policy are not defined by this NSA template.

Policy	Computer Setting
Enforce user logon restrictions	Not defined
Maximum lifetime for service ticket	Not defined
Maximum lifetime for user ticket	Not defined
Maximum lifetime for user ticket renewal	Not defined
Maximum tolerance for computer clock synchronization	Not defined

LOCAL POLICIES

Local policies include security settings that can be applied to individual computers. Policies defined here are set within the local computer account database. These policies consist of Audit Policy, User Rights Assignment, and Security Options.

Audit Policy

These policies determine the variety of audit settings Windows 2000 can record. These can be set for auditing successes, failures, or both. The settings defined under Audit Policy include the auditing of account logon events, account management, directory service access, logon events, object access, policy change, privilege use, process tracking, and system events.

Policy	Computer Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

Audit account logon events This monitors logon and logoff events validated by a domain controller, even if the access is to another computer. When enabled, events such as local logons to a workstation or remote logons to a server will be tracked. Since this template is being applied to a server in this situation, it will only track local account authentication access to the server. The NSA template has set "Audit account logon events" to audit for both success and failure.

Audit Account Management This monitors changes to the Security Accounts database. This includes creation, modification, and deletion of user accounts and groups, the enabling or disabling of user accounts, and the setting and resetting of passwords. Here the template has set "Audit Account Management" to audit for both success and failure.

Audit Directory Service Access This tracks user access to Active Directory objects that have their System Access Control List (SACL) defined. This is similar to Audit Object Access which depends on SACLs being set on NTFS objects, but Audit Directory Service Access audits only Active Directory objects. The W2K_Server template is configured to monitor for no auditing of directory service access.

Audit Logon Events This monitors logon and logoff events to the computer, including both interactive and network logon attempts. When applied to a server, as it will be in this case, this setting will audit all logon successes and/or logon failures on that particular workstation or server. When applied to a domain controller, this setting will be a subset of "Audit Account Logon Events." The

NSA template is configured to audit for both success and failure for “Audit Logon Events.”

Audit Object Access This tracks users’ access to NTFS objects that have their SACLs defined. Only when this setting is defined along with the SACL of an NTFS object will auditing begin. This then allows the individual auditing of different NTFS objects including folders, files, printers, and registry keys. This template has “Audit Object Access” defined for failure.

Audit Policy Change This monitors changes in security policy. This can include the altering of audit policy, user rights assignments, or trust policy. The NSA has configured “Audit Policy Change” for both success and failure in this template.

Audit Privilege Use This tracks the access to various privileged rights, which are user rights granted to Administrators and other power users. The user rights that are audited with this setting enabled are:

- Generate security audits
- Replace process level token
- Back up and Restore of files and directories
- Debug programs
- Create a token object
- Bypass traverse checking

The W2K_Server template defines “Audit Privilege Use” for failure.

Audit Process Tracking This monitors detailed program information such as executions, activations, and exits. Once enabled, this setting logs a large amount of data and can slow a system down. It is usually only enabled for debugging purposes for programmers. “Audit Process Tracking” is defined for no auditing in this Security Template.

Audit System Events This tracks events that affect the entire system such as startup and shutdown. This also monitors the clearing of the Audit log. The NSA has defined this setting within the W2K_Server template for both success and failure.

User Rights Assignment

These policies allow the setting of various rights for user accounts and security groups. A large portion of these settings are related to access to important security-related tasks. This section will only cover those "User Rights Assignment" settings that are defined within the W2K_Server template. If necessary, those undefined settings that should have been defined will be discussed within the analysis section.

Policy	Computer Setting
Access this computer from the network	Administrators,Users
Act as part of the operating system	
Add workstations to domain	
Back up files and directories	Administrators
Bypass traverse checking	Users
Change the system time	Administrators
Create a pagefile	Administrators
Create a token object	
Create permanent shared objects	
Debug programs	
Deny access to this computer from the network	
Deny logon as a batch job	
Deny logon as a service	
Deny logon locally	
Enable computer and user accounts to be trusted for dele...	
Force shutdown from a remote system	Administrators
Generate security audits	
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	
Log on as a service	
Log on locally	Administrators
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	
Replace a process level token	
Restore files and directories	Administrators
Shut down the system	Administrators
Synchronize directory service data	
Take ownership of files or other objects	Administrators

Access This Computer From The Network This setting establishes which users and groups are permitted to connect to the computer over the network. This

setting is defined for Administrators, Backup Operators, Power Users, Users, Everyone by default on servers. The NSA has configured Administrators and Users to have this right.

Act As Part Of The Operating System This setting permits a process to authenticate as any user and then acquire access to resources that a user has access. The server default defines this setting for the local system. This template defines this policy to no one.

Add Workstations To Domain This policy determines the users or groups that are authorized to add a workstation to the domain. This setting is only effective on Domain Controllers. The server default defines this setting for Authenticated Users. The NSA defines this policy for no one.

Backup Files And Directories This setting establishes what users and groups are permitted to back up files and directories. The specific permissions associated with this policy are:

- Read Attributes
- Read Extended Attributes
- List Folder/Read Data
- Traverse Folder/Execute File
- Read Permissions

The server default defines this setting for Administrators and Backup Operators. The W2K_Server template defines this policy for Administrators only.

Bypass Traverse Checking This setting establishes the users and groups that can traverse directory trees. This policy will be effective even if the user or group does not have rights on the traversed directory. This setting is defined for Administrators, Backup Operators, Power Users, Users, Everyone by default on servers. This template defines “Bypass Traverse Checking” for Users.

Change The System Time This setting controls the users and groups that can alter the time and date on the computer’s internal clock. The default setting for servers has this defined for Administrators and Power Users. The NSA template has this defined for Administrators only.

Create A Pagefile This setting governs the users and groups that are allowed to change the size of and create a pagefile. The W2K_Server template matches the default configuration for servers which both have this setting defined for Administrators.

Create A Token Object This setting establishes the users and groups that are allowed to be used by processes to generate a token that is then able to be used to gain access to local resources. The default for this setting on servers is Local

System. The NSA has configured this setting for Administrators within this template.

Create Permanent Shared Objects This setting controls the users and groups that are able to be utilized by processes to create a directory object. The default for this setting on servers is Local System. The W2K_Server template has this setting configured for no one.

Debug Programs This setting governs the users and groups that are allowed to attach a debugger to a process. The default for this policy on servers is Local System and Administrators. The NSA has defined this for no one within this template.

Deny Access To This Computer From The Network This policy establishes the users that are prohibited from accessing the computer over the network. When a user or group is subject to both "Access this computer from the network" and "Deny access to this computer from the network," the user or group will be denied access to the computer. The default for this setting on servers is Administrators, Backup Operators, Everyone, Users, and Power Users. This template has defined this policy for no one.

Deny Logon As A Batch Job This setting controls the accounts that are not permitted to logging on as a batch job. When "Log on as a batch job" and "Deny logon as a batch Job" are both applied to the same user or group, the user or group will be barred from logging on as a batch job. The default for this setting on a server and the NSA's configuration of this policy are both defined for no one.

Deny Logon As A Service This policy governs the service accounts or groups that are not allowed to register a process as a service. When a user or group is subject to both "Logon as a service" and "Deny logon as a service," the service account or group will be denied from logging on as a service. The default for servers for this setting is configured the same as this template, which are both defined for no one.

Deny Logon Locally This setting controls the users or groups that are prevented from logging on at a computer. When "Log on locally" and "Deny logon locally" are both applied to the same user or group, the user or group will be barred from logging on locally to the computer. The default for this setting on a server and the NSA's configuration of this policy are both defined for no one.

Enable Computer And User Accounts To Be Trusted For Delegation This policy dictates the users or groups that are allowed to configure the "Trusted for Delegation" setting on a computer or user object. The users or groups that are defined for this policy must also have write permissions to the user or computer

object's account control flags. The W2K_Server template has this setting configured for no one.

Force Shutdown From A Remote System This setting establishes the users and groups that are permitted to shut down a computer over the network from a remote location. This setting is defined for Administrators both within the default setting for this policy on servers and within the NSA's setting for this policy for this template.

Generate Security Audits This policy controls the users and groups that are able to be used by a process to insert entries into the security log. The default for this policy on servers is Local System. The NSA defines this policy for no one.

Increase Scheduling Priority This setting governs the users and groups that are allowed to use write property permissions to a process onto another process to raise the execution priority allocated to the other process. The default for this setting on servers is Administrators. This template also defines this policy for Administrators.

Load And Unload Device Drivers This policy dictates the users and groups that are allowed to dynamically load and unload device drivers. The default for this setting on servers is Administrators. The NSA also defines this policy for Administrators within this template.

Lock Pages In Memory This setting establishes the user and group accounts that are allowed to utilize a process to retain data in physical memory. This keeps the system from paging data to virtual memory. This setting is defined for no one both within the default setting for this policy on servers and within the NSA's setting for this policy within this template.

Log On As A Batch Job This setting controls the accounts that are permitted to log on as a batch job. When "Log on as a batch job" and "Deny logon as a batch Job" are both applied to the same user or group, the user or group will be barred from logging on as a batch job. The default for this setting on a server is Local System. The NSA's configuration of this policy is defined for no one.

Logon As A Service This policy governs the service accounts or groups that are allowed to register a process as a service. When a user or group is subject to both "Logon as a service" and "Deny logon as a service," the service account or group will be denied from logging on as a service. The default for servers for this setting is configured the same as this template, which are both defined for no one.

Log on Locally This setting controls the users or groups that are allowed to log on to a computer. When "Log on locally" and "Deny logon locally" are both applied to the same user or group, the user or group will be barred from logging on locally

on the computer. The default for this setting on a server includes the following groups: Administrators, Backup Operators, Power Users, Users, and Guests. The NSA's configuration of this policy for this template is defined for Administrators.

Manage Auditing And Security Log This policy establishes the users and groups that are allowed to configure object access auditing options for resources. The W2K_Server template matches the default configuration for servers that both have this setting defined for Administrators.

Modify Firmware Environment Values This setting controls the users and groups that are allowed to make changes to system-wide environment values. The default for this setting on a server is Local System and Administrators. The NSA's configuration of this policy is defined for only Administrators.

Profile Single Process This policy governs the users and groups that are permitted to monitor performance of non-system processes with performance monitoring tools. The default for this setting on a server is Local System and Administrators. The W2K_Server template configuration of this policy is defined for only Administrators.

Profile System Performance This setting dictates the users and groups that are allowed to monitor the performance of system processes with performance monitoring tools. The default for this setting on a server is Local System and Administrators. The NSA's configuration of this policy is defined for only Administrators.

Remove Computer From Docking Station This policy establishes the users and groups that are allowed to remove a portable computer from its docking station. The default for this setting on a server is Administrators, Power Users, and Users. The NSA's configuration of this policy within this template is defined for no one.

Replace A Process Level Token This setting controls the user and group accounts that are permitted to start a process to exchange the default token associated with a running sub-process. The default for this setting on a server is Local System. The NSA's configuration of this policy is defined for no one.

Restore Files And Directories This setting establishes what users and groups are permitted to restore files and directories. The default for this setting on a server is Backup Operators and Administrators. The W2K_Server template defines this policy for Administrators only.

Shutdown The System This policy governs the users and groups that are allowed to use the "Shut Down" command to shut down the operating system while logged on locally. The default for this setting on a server includes the following

groups: Administrators, Backup Operators, Power Users, and Users. The NSA's configuration of this policy for this template is defined for only Administrators.

Synchronize Directory Service Data This setting controls the users and groups that are permitted to synchronize directory service data. The default for servers for this setting is configured the same as this template, which are both defined for no one.

Take Ownership Of Files Or Objects This policy establishes the users and groups that have the authority to take ownership of securable objects within the system. This includes printers, registry keys, files and folders, processes, threads, and Active Directory objects. The default for this setting on servers is Administrators. The NSA also defines this policy for Administrators within this template.

Security Options

These policies cover a broad scope of security options that are managed by registry keys. These cover a diverse set of security settings. This section will only cover those "User Rights Assignment" settings that are defined within the W2K_Server template. If necessary, those undefined settings that should have been defined will be discussed within the analysis section.

Policy	Computer Setting
Additional restrictions for anonymous connections	No access without explicit anonymous permission
Allow server operators to schedule tasks (domain controll...	Not defined
Allow system to be shut down without having to log on	Disabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	30 minutes
Audit the access of global system objects	Enabled
Audit use of Backup and Restore privilege	Enabled
Automatically log off users when logon time expires	Not defined
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communication (always)	Disabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (always)	Disabled
Digitally sign server communication (when possible)	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Do not display last user name in logon screen	Enabled
LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NTLM
Message text for users attempting to log on	Not defined
Message title for users attempting to log on	Not defined
Number of previous logons to cache (in case domain contr...	0 logons
Prevent system maintenance of computer account password	Disabled
Prevent users from installing printer drivers	Enabled
Prompt user to change password before expiration	14 days
Recovery Console: Allow automatic administrative logon	Disabled
Recovery Console: Allow floppy copy and access to all dri...	Disabled
Rename administrator account	Not defined
Rename guest account	Not defined
Restrict CD-ROM access to locally logged-on user only	Enabled
Restrict floppy access to locally logged-on user only	Enabled
Secure channel: Digitally encrypt or sign secure channel d...	Disabled
Secure channel: Digitally encrypt secure channel data (wh...	Enabled
Secure channel: Digitally sign secure channel data (when ...	Enabled
Secure channel: Require strong (Windows 2000 or later) s...	Disabled
Secure system partition (for RISC platforms only)	Not defined
Send unencrypted password to connect to third-party SM...	Disabled
Shut down system immediately if unable to log security au...	Enabled

Additional Restrictions For Anonymous Connections This policy establishes what extra restrictions will be placed on anonymous computer connections. This can be configured as:

- None. Rely on default permissions.
- Do not allow enumeration of SAM accounts and shares – Security Permissions for resources have the "Authenticated Users" group replace the "Everyone" group.
- No access without explicit anonymous permissions – "Network" and "Everyone" are removed from the anonymous users token

Windows 2000 Servers rely on the default permissions. The W2K_Server Template configures this setting with "No access explicit anonymous permissions."

Allow System To Be Shut Down Without Having To Log On This policy controls whether a user or group will be able to shut down Windows without logging on first. When this setting is enabled, the Shutdown option appears on the Log On screen, whereas if it's disabled, the Shutdown option will not appear. The default for servers and the W2K_Server template both disable this setting.

Allowed To Eject Removable NTFS Media This setting establishes who is allowed to eject removable NTFS Media. The default for this setting on a server is enabled for Administrators only. The W2K_Server template also defines this policy for Administrators.

Amount Of Idle Time Required Before Disconnecting Session This policy dictates the extent of continuous idle time that is required to be exceeded in a Server Message Block session before the session is disconnected because of inactivity. A value of 0 will disconnect the session as soon as possible. The maximum value this setting can take is 99,999 minutes. The default for servers for this setting is 15 minutes. The NSA defines this setting at 30 minutes in this template.

Audit The Access Of Global System Objects This setting dictates whether access to global system objects will be audited. When this setting is enabled objects such as events, mutexes, semaphores and DOS devices are produced with a default SACL. This policy must be enabled along with "Audit object access" to audit access to these system objects. The default for this setting on a server is disabled. The W2K_Server template defines this policy as enabled.

Audit The Use Of Backup And Restore Privilege This policy controls whether the use of all user privileges will be audited, as well as Backup and Restore. In order to produce an audit event each time a directory or file is backed up or restored, this setting must be enabled with "Audit Privilege Use" defined as well. The default for this setting on a server is disabled. The W2K_Server template defines this policy as enabled.

Automatically Log Off Users When Logon Time Expires (Local) This policy establishes whether users will be disconnected when connected to local machines outside of their valid logon hours. This setting is enabled by default on Windows 2000 Servers. The NSA's template enables this setting as well.

Clear Virtual Memory Pagefile When System Shuts Down This setting controls whether the virtual memory pagefile is erased when the system shuts down. Virtual memory writes pages of memory to disk. If this setting is disabled, after a system is shutdown, this virtual memory could be accessed by another operating system. The default for this setting on a server is disabled. The W2K_Server template defines this policy as enabled.

Digitally Sign Client Communication (Always) This policy establishes whether the SMB client component requires packet signing. When this setting is enabled, the Microsoft server must perform SMB packet signing in order to communicate with the Microsoft client. However, when this policy is disabled, the client and the server will negotiate SMB packet signing. The server default and the W2K_Server template both have this setting disabled.

Digitally Sign Client Communication (When Possible) This setting dictates whether the SMB client component will try packet signing with the server. When this setting is enabled and packet signing is enabled on the server, the Microsoft server will perform SMB packet signing in order to communicate with the Microsoft client. However, when this policy is disabled, the client will not negotiate SMB packet signing. The server default and the W2K_Server template both have this setting enabled.

Digitally Sign Server Communication (Always) This policy governs whether the SMB server component requires packet signing. When this setting is enabled, the Microsoft client must perform SMB packet signing in order to communicate with the Microsoft server. However, when this policy is disabled, the client and the server will negotiate SMB packet signing. The server default and the W2K_Server template both have this setting disabled.

Digitally Sign Server Communication (When Possible) This setting establishes whether the SMB server component will try packet signing with the client. When this setting is enabled and packet signing is enabled on the client, the Microsoft client will perform SMB packet signing in order to communicate with the Microsoft server. However, when this policy is disabled, the server will not negotiate SMB packet signing. The server default and the W2K_Server template both have this setting enabled.

Disable CTRL+ALT+DEL Requirement For Logon Screen This policy controls whether it is necessary for a user to hold down the CTRL+ALT+DEL keys on the keyboard to log on. When this policy is enabled, users do not have to press the CTRL+ALT+DEL keys. When it is disabled, users are forced to press

CTRL+ALT+DEL to be able to log on. This is disabled by default on servers and is also disabled on the NSA's template.

Do Not Display Last User Name In Logon Screen This setting establishes whether the logon name of the last user to log on to the system will be viewable on the Windows logon screen. When this policy is disabled, the last user to successfully log on will be displayed on the Windows logon screen. When the policy is disabled, the last successful logon name will not appear. This is disabled by default on Windows 2000 Servers, but is enabled on the NSA's W2K_Server template.

LAN Manager Authentication Level This policy dictates the challenge/response authentication protocol that is applied for network logons. This setting influences the degree of session security, as well as the levels of authentication security used by clients and accepted by servers. The following is the various settings this policy can take:

- Send LM & NTLM responses: LM, NTLM, and NTLMv2 authentication is accepted by domain controllers. LM and NTLM authentication is accepted by clients. NTLMv2 is never used by clients.
- Send LM & NTLM - use NTLMv2 session security if negotiated: LM, NTLM, and NTLMv2 authentication is accepted by domain controllers. LM and NTLM authentication is used by clients. NTLMv2 is used by clients if the server supports it.
- Send NTLM response only: LM, NTLM, and NTLMv2 authentication is accepted by domain controllers. NTLM authentication is used by clients. NTLMv2 is used by clients if the server supports it
- Send NTLMv2 response only: LM, NTLM, and NTLMv2 authentication is accepted by domain controllers. NTLMv2 is exclusively used for authentication by clients. NTLMv2 is used for session security by clients if the server supports it.
- Send NTLMv2 response only\refuse LM: LM is refused by domain controllers. NTLM and NTLMv2 are accepted by domain controllers. NTLMv2 is exclusively used for authentication by clients. NTLMv2 is used for session security by clients if the server supports it.
- Send NTLMv2 response only\refuse LM & NTLM: LM and NTLM are refused by domain controllers. Domain controllers only accept NTLMv2 authentication. NTLMv2 is exclusively used for authentication by clients. NTLMv2 is used for session security by clients if the server supports it.

Send LM & NTLM responses is the server default for this setting. The NSA has configured the W2K_Server template with "Send NTLMv2 response only\refuse LM & NTLM."

Number Of Previous Logons To Cache This setting controls how many times a user is able to log on to a Windows domain with cached account information.

When a workstation or server is offline, or when a domain controller is unreachable, this setting caches all previous users' logons. A value of 0 will disable logon caching. Although this can be set above 50, it will only cache a maximum of 50 logon attempts. The server default for this setting is 10 logons. The W2K_Server template has this setting configured for 0 logons.

Prevent System Maintenance Of Computer Account Password This policy establishes whether member computers will be refused when requesting new computer account passwords from domain controllers. By default, computer account passwords are changed every 30 days by member computers. When this setting is enabled, domain controllers deny computer account password change requests. This setting is disabled by default on servers and on the W2K_Server template.

Prevent Users From Installing Printer Drivers This setting dictates whether users can install printer drivers when adding a network printer. If this setting is disabled, only Power Users and Administrators are able to install printer drivers when adding a network printer. When this setting is enabled, any user is able to install printer drivers when adding a network printer. The server default for this setting is enabled. The NSA's template also configures this setting as enabled.

Prompt User To Change Password Before Expiration This policy governs the number of days ahead of time users will be warned that their password is going to expire. The server default for this setting is 14 days. The W2K_Server template also configures this setting at 14 days.

Recovery Console: Allow Automatic Administrative Logon This setting dictates whether the Administrator account password must be given in order to access the Recovery Console. When this setting is enabled, users can log on to the Recover Console without a password. When it is disabled, a password is required to log on to the Recovery Console. This setting is disabled by default on servers and as configured in this template.

Recovery Console: Allow Floppy Copy And Access To All Drives And All Folders This policy allows users to set certain environment variables by making available the Recovery Console SET command. When this is enabled, the environment variables can be set to enable wildcard support on certain commands, access can be granted to all files and folders on the computer, and files can be copied to removable media. The default server setting for this policy is disabled. The W2K_Server template also has this setting disabled.

Restrict CD-ROM Access To Locally Logged-On User Only This policy establishes whether both local and remote users can access a CD-ROM at the same time. When this policy is enabled and a user is interactively logged on, only that interactively logged on user can access the CD-ROM. When this setting is enabled, the CD-ROM can be accessed over the network only when no

users are interactively logged on. The server default for this setting is disabled. This setting is enabled on the NSA's template.

Restrict Floppy Access To Locally Logged-On User Only This setting controls whether both local and remote users can access a floppy disk at the same time. When this policy is enabled and a user is interactively logged on, only that interactively logged on user can access the floppy disk. When this setting is enabled, the floppy disk can be accessed over the network only when no users are interactively logged on. The server default for this setting is disabled. This setting is enabled on the NSA's template.

Secure Channel: Digitally Encrypt Or Sign Secure Channel Data (Always) This policy establishes whether all secure channel traffic has to be signed or encrypted when initiated by the domain member. When this setting is enabled, either signing or encryption of all secure channel traffic must be negotiated for the secure channel to be established. When this setting is disabled, the encryption and signing for secure channel traffic is negotiated with the Domain Controller. This setting is enabled by default on servers. The W2K_Server template disables this setting.

Secure Channel: Digitally Encrypt Secure Channel Data (When Possible) This setting controls whether a member computer, when initiating secure channel traffic, attempts to negotiate encryption. When this is enabled domain members will request that all secure channel traffic be encrypted. When this setting is disabled, the domain member will not try to negotiate secure channel encryption. This setting is enabled by default on servers and is enabled in the NSA's template as well.

Secure Channel: Digitally Sign Secure Channel Data (When Possible) This policy establishes whether a member computer, when initiating secure channel traffic, attempts to negotiate signing. When this is enabled, domain members will request that all secure channel traffic be signed. When this setting is disabled the domain member will not request the signing of secure channel traffic. This setting is enabled by default on servers and is enabled in the NSA's template as well.

Secure Channel: Require Strong (Windows 2000 Or Later) Session Key This setting dictates whether secure channel data requires 128-bit key strength for encryption. When this setting is enabled, the secure channel will only be established when 128-bit encryption can be performed. When this setting is disabled, the domain controller will negotiate key strength. This setting is disabled by default on servers. The W2K_Server template also disables this setting.

Send Unencrypted Password To Connect To Third-party SMB Servers This setting determines whether plaintext passwords can be sent by the Server

Message Block (SMB) redirector to third-party SMB servers that do not handle encrypted passwords when authenticating. When this policy is enabled, the SMB is allowed to send plaintext passwords. When this setting is disabled, the SMB only sends encrypted passwords. This policy is disabled by default on Windows 2000 servers and is also disabled within this template.

Shut Down System Immediately If Unable To Log Security Audits When the system is unable to log security events, this policy controls whether the system will shut down or continue running. When this setting is enabled, the system will stop if a security audit cannot be logged, no matter what the reason. This setting is disabled by default on servers. The W2K_Server template enables this setting.

Smart Card Removal Behavior This setting dictates the possible results of removing a smart card from a smart card reader while a user is logged on. This policy can be configured with three possible settings:

- No Action – the user remains logged on when the smart card is removed from the reader.
- Lock Workstation – the workstation is locked when the smart card is removed from the reader.
- Force Logoff – the user is automatically logged off when the smart card is removed from the reader.

This setting is configured to "No Action" by default on servers. The NSA's template sets this policy to "Lock Workstation."

Strengthen Default Permissions Of Global System Objects This policy controls the strength of the default discretionary access control list (DACL) for objects. The default DACL is stronger when this policy is enabled. Non-administrative users are not allowed to modify shared objects they did not create when this setting is enabled. The default server setting for this policy is enabled. The NSA's template also has this configured as enabled.

Unsigned Driver Installation Behavior This setting establishes the consequences of installing a device driver that has not been Windows certified by the Windows Hardware Quality Lab (WHQL). The possible settings for this are:

- Silently succeed – the driver will install without warning.
- Warn but allow installation – the user will be warned that the driver has not been WHQL certified, but the user will be allowed to continue the installation.
- Do not allow installation – the user will not be allowed to install the driver.

The server default for this setting is "Warn but allow installation." The W2K_Server template configures this setting to "Warn but allow installation."

Unsigned Non-Driver Installation Behavior This policy governs the consequences of installing a non-device driver that has not been Windows certified by the Windows Hardware Quality Lab (WHQL). The possible settings for this are:

- Silently succeed – the driver will install without warning.
- Warn but allow installation – the user will be warned that the driver has not been WHQL certified, but the user will be allowed to continue the installation.
- Do not allow installation – the user will not be allowed to install the driver.

The server default for this setting is "Silently Succeed." The W2K_Server template also configures this setting to "Warn but allow installation."

Event Log

The last of the Local Policy sections controls various aspects of the Event Log. This section will only cover those "Event Log" settings that are defined within the W2K_Server template. If necessary, those undefined settings that should have been defined will be discussed within the analysis section.

Policy	Computer Setting
Maximum application log size	4194240 kilobytes
Maximum security log size	4194240 kilobytes
Maximum system log size	4194240 kilobytes
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retain application log	Not defined
Retain security log	Not defined
Retain system log	Not defined
Retention method for application log	Manually
Retention method for security log	Manually
Retention method for system log	Manually
Shut down the computer when the security audit log is full	Enabled

Maximum Application Log Size This policy identifies the application event log's maximum size. The largest this can be is 4 Gigabytes. The server default for this setting is 512 kilobytes. The W2K_Server template sets this at 4,194,240 kilobytes.

Maximum Security Log Size This setting identifies the security event log's maximum size. The largest this can be is 4 Gigabytes. The server default for this setting is 512 kilobytes. The W2K_Server template sets this at 4,194,240 kilobytes.

Maximum System Log Size This policy identifies the system event log's maximum size. The largest this can be is 4 Gigabytes. The server default for this setting is 512 kilobytes. The W2K_Server template sets this at 4194240 kilobytes.

Prevent Local Guests Group From Accessing Application Log This setting establishes whether the application event log will be accessible to guests. The setting is disabled by default on servers, allowing local guests to access the application log. This setting is enabled on the NSA's template, preventing guests from accessing the log.

Prevent Local Guests Group From Accessing Security Log This policy controls whether the security event log will be accessible to guests. The setting is "disabled" by default on servers, allowing local guests to access the security log. This setting is enabled on the NSA's template, preventing guests from accessing the log.

Prevent Local Guests Group From Accessing System Log This setting dictates whether the system event log will be accessible to guests. The setting is "disabled" by default on servers, allowing local guests to access the system log. This setting is enabled on the NSA's template, preventing guests from accessing the log.

Retain Application Log This policy establishes how many days' worth of events the application log will save when the retention method for the application log is " Overwrite Events By Days." The Windows 2000 Server default for this setting is "none". The W2K_Server template configures this to "7 days."

Retain Security Log This setting controls how many days' worth of events the security log will save when the retention method for the security log is "Overwrite Events By Days." The Windows 2000 Server default for this setting is "none". The W2K_Server template configures this to "7 days."

Retain System Log This policy governs how many days' worth of events the system log will save when the retention method for the system log is " Overwrite Events By Days." The Windows 2000 Server default for this setting is "none". The W2K_Server template configures this to "7 days."

Retention Method For Application Log This setting establishes the process for retaining the application log. There are three choices:

- Overwrite events by day – Events are overwritten by the number of days specified in the "Retain Application Log" setting.
- Overwrite events as needed – This automatically overwrites old logs as the "Maximum Application Log" size is reached

- Do not overwrite events (clear logs manually) – This requires the logs to be cleared manually. When the "Maximum Application Log" size is reached, new events are not recorded.

The server default for this setting is "none." The W2K_Server template defines this setting with "Do not overwrite events (clear logs manually)."

Retention Method For Security Log This policy controls the process for retaining the security log. There are three choices:

- Overwrite events by day – Events are overwritten by the number of days specified in the "Retain Security Log" setting.
- Overwrite events as needed – This automatically overwrites old logs as the "Maximum Security Log" size is reached
- Do not overwrite events (clear logs manually) – This requires the logs to be cleared manually. When the "Maximum Security Log" size is reached, new events are not recorded.

The server default for this setting is "none." The W2K_Server template defines this setting with "Do not overwrite events (clear logs manually)."

Retention Method For System Log This setting establishes the process for retaining the system log. There are three choices:

- Overwrite events by day – Events are overwritten by the number of days specified in the "Retain System Log" setting.
- Overwrite events as needed – This automatically overwrites old logs as the "Maximum System Log" size is reached
- Do not overwrite events (clear logs manually) – This requires the logs to be cleared manually. When the "Maximum System Log" size is reached, new events are not recorded.

The server default for this setting is "none." The W2K_Server template defines this setting with "Do not overwrite events (clear logs manually)."

RESTRICTED GROUPS

The Restricted Groups Policy enforces group membership, implementing both who is a member of a group and who is not a member of a group. There are two properties that can be defined within Restricted Groups. The "Members of this group" property defines groups that will be members of the restricted group. The "This group is a member of" property defines groups to which the restricted group will belong. Any group that is defined as a member of a Restricted Group will be forced into that restricted group. Any group not defined within a Restricted Group will be forced out of the group. The server default has nothing configured for this

policy. Power Users are defined as a restricted group within the W2K_Server template. It enforces no groups as a member of Power Users, nor does it specify Power Users as a member of any other group.

SYSTEM SERVICES

This policy defines system service configuration. It allows the startup mode for system services to be defined as manual, automatic, or disabled. The setting also defines possible access permissions including start, stop, and pause for system services. This policy is undefined both as the server default and within the W2K_Server template.

REGISTRY

This policy configures Discretionary Access Control Lists (DACLs) and System Access Control Lists (SACLS) for registry settings. The server default leaves this policy undefined. The W2K_Server Template secures many critical and sensitive keys. More detail on these settings can be found in **Appendix A**.

Object Name	Permission	Audit
CLASSES_ROOT	Replace	Replace
machine\software	Replace	Replace
machine\software\microsoft\netdde	Replace	Replace
MACHINE\SOFTWARE\Microsoft\OS/2 ...	Replace	Replace
machine\software\microsoft\protected...	Ignore	Ignore
MACHINE\SOFTWARE\Microsoft\Wind...	Replace	Replace
machine\software\microsoft\windows ...	Replace	Replace
machine\software\microsoft\windows\...		
machine\software\microsoft\windows\...		
machine\software\microsoft\windows\...		
machine\system	Replace	Replace
machine\system\clone	Ignore	Ignore
machine\system\controlset001		
machine\system\controlset002		
machine\system\controlset003		
machine\system\controlset004		
machine\system\controlset005		
machine\system\controlset006		
machine\system\controlset007		
machine\system\controlset008		
machine\system\controlset009		
machine\system\controlset010		
machine\system\currentcontrolset\con...	Replace	Replace
machine\system\currentcontrolset\con...	Replace	Replace
machine\system\currentcontrolset\enum	Ignore	Ignore
machine\system\currentcontrolset\har...		
MACHINE\SYSTEM\CurrentControlSet\...	Replace	Replace
MACHINE\SYSTEM\CurrentControlSet\...	Replace	Replace
users\.default	Replace	Replace
users\.default\software\microsoft\net...	Replace	Replace
users\.default\software\microsoft\pro...	Ignore	Ignore

FILE SYSTEM

This policy configures Discretionary Access Control Lists (DACLs) and System Access Control Lists (SACLS) for the file system. The server default leaves this policy undefined. The W2K_Server Template's registry settings can be found in **Appendix B**.

Object Name	Permission	Audit
%ProgramFiles%	Replace	Replace
%SystemDirectory%	Replace	Replace
%SystemDirectory%\appmgmt		
%SystemDirectory%\config	Replace	Replace
%SystemDirectory%\dllcache	Replace	Replace
%SystemDirectory%\DTCLog		
%SystemDirectory%\GroupPolicy		
%SystemDirectory%\ias	Replace	Replace
%SystemDirectory%\Ntbackup.exe	Replace	Replace
%SystemDirectory%\NTMSData		
%SystemDirectory%\rcp.exe	Replace	Replace
%SystemDirectory%\regedt32.exe	Replace	Replace
%SystemDirectory%\ReinstallBackups	Ignore	Ignore
%SystemDirectory%\repl		
%SystemDirectory%\repl\export		
%SystemDirectory%\repl\import		
%SystemDirectory%\rexec.exe	Replace	Replace
%SystemDirectory%\rsh.exe	Replace	Replace
%SystemDirectory%\secedit.exe	Replace	Replace
%SystemDirectory%\Setup		
%SystemDirectory%\spool\printers	Replace	Replace
%SystemDrive%\		
%SystemDrive%\autoexec.bat	Replace	Replace
%SystemDrive%\boot.ini	Replace	Replace
%SystemDrive%\config.sys	Replace	Replace
%SystemDrive%\Documents and Setti...		
%SystemDrive%\Documents and Setti...	Replace	Replace
%SystemDrive%\Documents and Setti...		
%SystemDrive%\Documents and Setti...	Replace	Replace
%SystemDrive%\Documents and Setti...	Replace	Replace
%SystemDrive%\Documents and Setti...	Replace	Replace
%SystemDrive%\Inetpub	Ignore	Ignore
%SystemDrive%\IO.SYS	Replace	Replace
%SystemDrive%\MSDOS.SYS	Replace	Replace
%SystemDrive%\My Download Files	Replace	Replace
%SystemDrive%\ntdetect.com	Replace	Replace

APPLYING THE TEMPLATE

The W2K_Server template will be applied throughout the enterprise using group policy. It will be applied across all member server Organizational Units (OUs). For this particular case, the W2K_Server template will be applied to the "Options" OU under the "Member Servers" OU. The template will be imported into the OU Group Policy by:

1. Enter the Properties of the OU
2. Edit the Group Policy
3. Expand the Policy Object
4. Expand Computer Configuration
5. Expand Windows Settings
6. In the console tree, right-click Security Settings
7. Click Import Policy
8. Choose the W2K_Policy

The Group Policy will be refreshed by the default of every 90 minutes, with a plus/minus of up to 30 minutes.

Group Policy was chosen as the application method because the deployment of the W2K_Server Template can be automated to multiple servers by applying it to a single OU. That Group Policy can then be linked to many other OUs across the enterprise. A single change to the one Group Policy will then be automatically updated through the linking and Group Policy refreshes.

Additionally, different tools would be used to maintain the template and Group Policy. Secedit.exe would be to refresh Group Policy using Secedit's /refreshpolicy command-line switch and to check the template for errors using Secedit's /validate command-line switch. The template will be compared to other Security Templates using the Security and Configuration tool. This will be useful to compare settings on another system to those of the template.

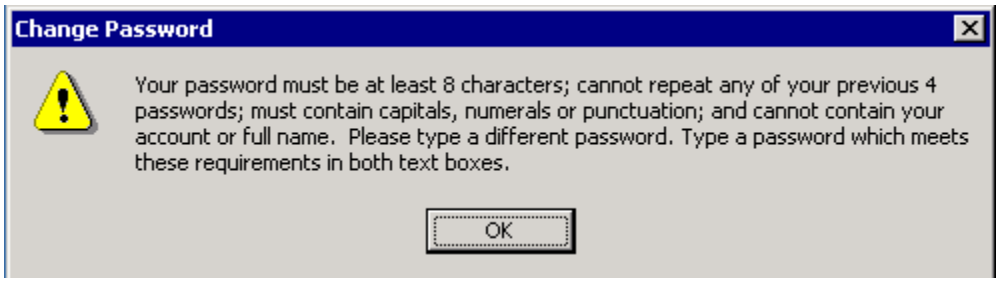
TESTING THE TEMPLATE

This section will test the Security Template to demonstrate that the template has been applied properly and that the settings function as anticipated. The first two tests will assess password policy and account lockout policy. As discussed earlier, password policy set at the OU level will not be effective for domain user accounts. Domain user account policy will be defined by the default domain policy which is implemented by the domain controllers within the domain. This template will still affect local security policy, so these tests will focus on local user accounts. The rest of the tests will focus on audit policy.

Test 1: Verifying Password GPO is Applied

Test Procedures: Password Policy

1. Log on as Administrator using a correct password.
    a. Enter the Username Administrator
    b. Enter the correct password
2. Change the date of the Server to 91 days from today.
    a. Right-click the date.
    b. Choose Adjust Date & Time from the dropdown box
    c. Use the Date dropdown box to adjust the date forward three months and 1 day.
3. Log off of the Server.
    a. Click Start | Shutdown
    b. Choose Log off
    c. Click OK.
4. Log on as Local_Test_User_1
    a. Enter Username
    b. Enter Password
5. Local_Test_User_1 will be prompted to change its password. Change Local_Test_User_1's password as prompted.
    a. Use a blank password. This fails with the message below.
    b. Try using a password of 11 characters including upper and lower case letters and a number. This fails.
    c. Try using a 12 character password with no letters. This fails.
    d. Try using the previous password. This fails.



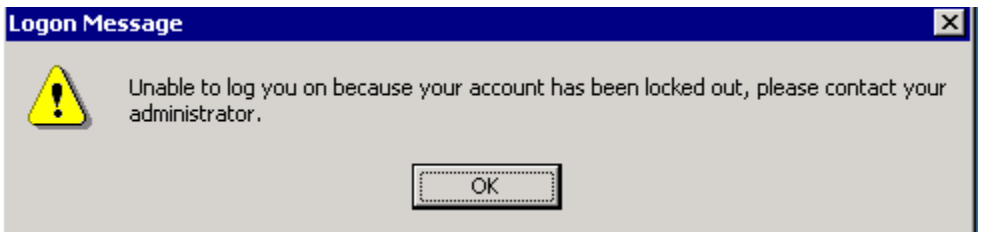
Test Analysis: Password Policy

This tested various settings within the Password Policy. It first verified the "Maximum password age" by changing the date of the server to 91 days into the future and the user was forced to change her password. Next the test validates "Minimum password length" by attempting to set a password at less than 12 characters and being denied. The test then checks the "Password must meet complexity requirements" by being denied when entering a password with no letters. The test also touches on the "Enforce password history" setting when the user is unable to set her password using her previous password.

Test 2: Verifying Account Lockout Policy Is Applied Accurately

Test Procedures: Account Lockout Policy

1. Log off of the Server.
    a. Click Start | Shutdown
    b. Choose Log off, Click OK
2. Log on using an incorrect password.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Local_Test_User_1
    c. Enter an incorrect password.
3. Log on using an incorrect password.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Local_Test_User_1
    c. Enter an incorrect password.
4. Log on using an incorrect password.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Local_Test_User_1
    c. Enter an incorrect password.
5. Log on using the correct password.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Local_Test_User_1
    c. Enter the correct password.
    d. This is unsuccessful as the Account Lockout threshold has been reached.



6. Log on as Administrator using a correct password.
    a. Enter the Username Administrator
    b. Enter the correct password
7. On a Server, open the Microsoft Management Console.
    a. Click Start | Run
    b. Type mmc in the Run window
    c. Click OK.
8. Add the Computer Management snap-in.
    a. Click Console | Add/Remove Snap-in
    b. Click Add
    c. Choose Computer Management
    d. Click Add.
    e. Click OK.
9. Enter Local_Test_User_1's account properties and unlock the account
    a. Click the Users container.
    b. Right-Click on Local_Test_User_1 and choose Properties from the drop-down box.
    c. Clear the Account Locked checkbox.
10. Log off of the Server.
    a. Click Start | Shutdown
    b. Choose Log off
    c. Click OK
11. Log on using an incorrect password.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Local_Test_User_1
    c. Enter an incorrect password.
12. Log on using an incorrect password.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Local_Test_User_1
    c. Enter an incorrect password.
13. Wait 16 minutes.
14. Log on using an incorrect password.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Local_Test_User_1
    c. Enter an incorrect password.
15. Log on using an incorrect password.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Local_Test_User_1
    c. Enter an incorrect password.
16. Log on using a correct password. This is successful as the account lockout counter was reset.
17. Log off of the Server.
    a. Click Start | Shutdown
    b. Choose Log off
    c. Click OK

18. Log on using an incorrect password.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Local_Test_User_1
    c. Enter an incorrect password.
19. Log on using an incorrect password.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Local_Test_User_1
    c. Enter an incorrect password.
20. Log on using an incorrect password.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Local_Test_User_1
    c. Enter an incorrect password.
21. Log on using the correct password.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Local_Test_User_1
    c. Enter the correct password.
    d. This is unsuccessful as the Account Lockout threshold has been reached.
22. Wait 16 minutes
23. Log on using a correct password. This is successful as the account lockout duration has passed reset.

Test Analysis: Account Lockout Policy

This tested various settings within the Account Lockout Policy. It first verified the "Account lockout threshold" by unsuccessfully attempting to log on with the wrong password three times. When the user tried to log on with the correct password, the user was denied because he reached the account lockout threshold. Next the test validated "Reset account lockout counter after" by unsuccessfully attempting to log on with the wrong password two times, waiting 16 minutes, once again attempting to log on with the incorrect password two more times, then successfully logging on with the correct password. The user was not locked out because the account lockout counter had reset. Finally, the test then checks the "Account lockout duration" by locking the account out through attempting to log on with the incorrect password, then waiting 16 minutes and successfully logging on. The account lockout duration had been reached, unlocking the users account.

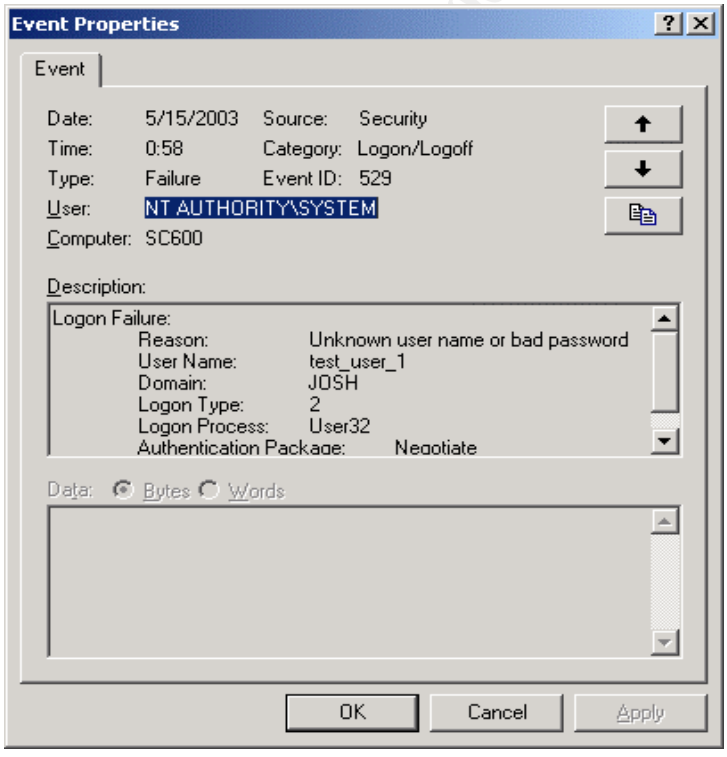
Test 3: Verifying Security Events Are Audited Accurately

Test Procedures: Audit Logon Events

1. Log off of the Server.
    a. Click Start | Shutdown
    b. Choose Log off

c. Click OK

2. Log on using an incorrect password.
   a. Press Ctrl-Alt-Del to bring up the Login Window
   b. Enter the Username Test_User_1
   c. Enter an incorrect password.
3. Log on using a correct password.
   a. Enter the Username Administrator
   b. Enter the correct password
4. On a Server, open the Microsoft Management Console.
   a. Click Start | Run
   b. Type mmc in the Run window
   c. Click OK.
5. Add the Event Viewer.
   a. Click Console | Add/Remove Snap-in
   b. Click Add
   c. Choose Event Viewer and Click OK
   d. Accept the default Local Computer by clicking Finish
   e. Click OK.
6. Check the Event Security Logs and confirm that logon and logoff events were recorded properly.
   a. Verify a Failure Audit exists for Login/Logoff from the failed login by double-clicking the most recent events.
   b. Verify a Success Audit exists for Login/Logoff from the successful login by double clicking the most recent events.
   c. Click OK after viewing each audit.



Test Analysis: Audit Logon Events

This test verified success and failure audits for the "Audit logon events" setting within the audit policies. It had a user first attempt to log on with an incorrect password and then had the user successfully log on. It then verified an audit was recorded for both the failure and the success in the Security Event Logs.

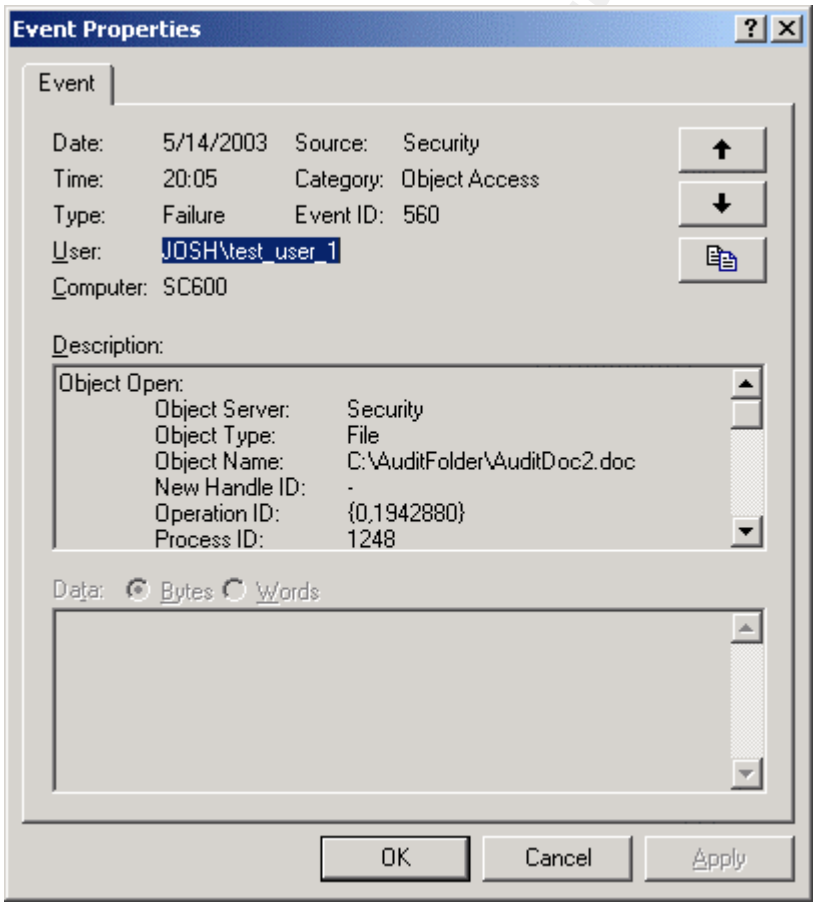
Test Procedures: Audit Object Access – Files and Folders

1. Log on as administrator.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Administrator
    c. Enter the password
2. Create a New Folder
    a. Right-click on an empty desktop space
    b. Choose New | Folder from the drop-down box
    c. Name the folder 'AuditFolder'
3. Create a Text Document in 'AuditFolder'.
    a. Double-click 'AuditFolder' to open it
    b. Right-click within the open folder
    c. Choose New | Test Document from the drop-down box
    d. Name the document 'AutitDoc'
4. Create another Text Document in 'AuditFolder'.
    a. Right-click within the open folder
    b. Choose New | Test Document from the drop-down box
    c. Name the new document 'AuditDoc2'
5. Deny Test_User_1 access to AuditDoc2.
    a. Right-click on AuditDoc2.
    b. Choose Properties from the drop-down list.
    c. Click on the Security tab.
    d. Click Add
    e. Scroll down and click on Test_User_1
    f. Click OK
    g. Click on Deny Access for Full Control
    h. Click OK
6. Enter the audit properties of AuditFolder.
    a. Right-click on AuditFolder
    b. Choose Properties from the drop-down menu
    c. Click the Security tab
    d. Click the Advanced Features pushbutton
    e. Click on the Audit Tab
7. Add Test_User_1
    a. Click the Add pushbutton
    b. Scroll down and Click Test_User_1
    c. Click OK

8. Choose to audit Test_User_1 for Success for Create Files/Write Data and Create Folders/Append Data.
    a. Click the Success and Failure check boxes for Create Files/Write Data
    b. Click the Success and Failure check boxes for Create Folders/Append Data
    c. Click the Apply onto child objects checkbox
9. Enter the audit properties of AuditDoc.
    a. Right-click on AuditDoc
    b. Choose Properties from the drop-down menu
    c. Click the Security tab
    d. Click the Advanced Features pushbutton
    e. Click on the Audit tab
10. Add Test_User_1
    a. Click the Add pushbutton
    b. Scroll down and Click Test_User_1
    c. Click OK
11. Choose to audit Test_User_1 for Success for Create Files/Write Data and Create Folders/Append Data.
    a. Click the Success and Failure check boxes for Create Files/Write Data
    b. Click the Success and Failure check boxes for Create Folders/Append Data
    c. Click the Apply onto child objects checkbox
12. Enter the audit properties of AuditDoc2.
    a. Right-click on AuditDoc2
    b. Choose Properties from the drop-down menu
    c. Click the Security tab
    d. Click the Advanced Features pushbutton
13. Log off of the Server.
    a. Click Start | Shutdown
    b. Choose Log Off and Click OK
14. Log on Test_User_1.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Test_User_1
    c. Enter the password
15. Open AuditFolder and AuditDoc.
    a. Double-click AuditFolder to open it
    b. Double-click the Text Document
    c. Type “hello” on the top line of the Text Document.
    d. Click File | Save to save the document.
16. Attempt to open AuditDoc2.
    a. Double-click AuditDoc2
    b. Access should be denied.
17. Log off of the Server.
    a. Click Start | Shutdown

b. Choose Log Off
c. Click OK

18. Log on as administrator.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Administrator
    c. Enter the password
19. On a Server, open the Microsoft Management Console.
    a. Click Start | Run
    b. Type mmc in the Run window
    c. Click OK.
20. Add the Event Viewer Snap-in.
    a. Click Console | Add/Remove Snap-in
    b. Click Add
    c. Choose Event Viewer and Click OK
    d. Accept the default Local Computer by clicking Finish
    e. Click OK.
21. Check the Event Security Logs and confirm that the object access events were recorded properly.
    a. Verify a Failure Audit exists for object access of Auditdoc2 from the document by double clicking the most recent events.



22. Enter the audit properties of AuditFolder.
    a. Right-click on AuditFolder
    b. Choose Properties from the drop-down menu
    c. Click the Security tab
    d. Click the Advanced Features pushbutton
23. Add Test_User_1
    a. Click the Add pushbutton
    b. Scroll down and Click Test_User_1
    c. Click OK
24. Discontinue auditing Test_User_1 for Success for Create Files/Write Data and Create Folders/Append Data.
    a. Clear the Success and Failure check boxes for Create Files/Write Data
    b. Clear the Success and Failure check boxes for Create Folders/Append Data
25. Repeat 22-25 for AuditDoc and AuditDoc2
26. Log off of the Server
    a. Click Start | Shutdown
    b. Choose Log Off
    c. Click OK
27. Log on Test_User_1.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Test_User_1
    c. Enter the password
    d. Open, alter, and save the text document.
28. Open AuditFolder and AuditDoc.
    a. Double-click AuditFolder to open it
    b. Double-click the Text Document
    c. Type “goodbye” on the top line of the Text Document.
    d. Click File | Save to save the document.
29. Attempt to open AuditDoc2.
    a. Double-click AuditDoc2
    b. Access should be denied.
30. Log off of the Server.
    a. Click Start | Shutdown
    b. Choose Log Off
    c. Click OK
31. Log on as administrator.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Administrator
    c. Enter the password
32. On a Server, open the Microsoft Management Console.
    a. Click Start | Run
    b. Type mmc in the Run window
    c. Click OK.
33. Add the Local Policy Snap-in.

a. Click Console | Add/Remove Snap-in
b. Click Add
c. Choose Event Viewer
d. Click OK
e. Accept the default Local Computer by clicking Finish
f. Click OK.

34. Check the Event Security Logs and confirm that the object access events were not audited as the object audits were removed.
    a. Double-click the most recent events and verify no object access logs exist.
    b. Click OK after viewing each audit

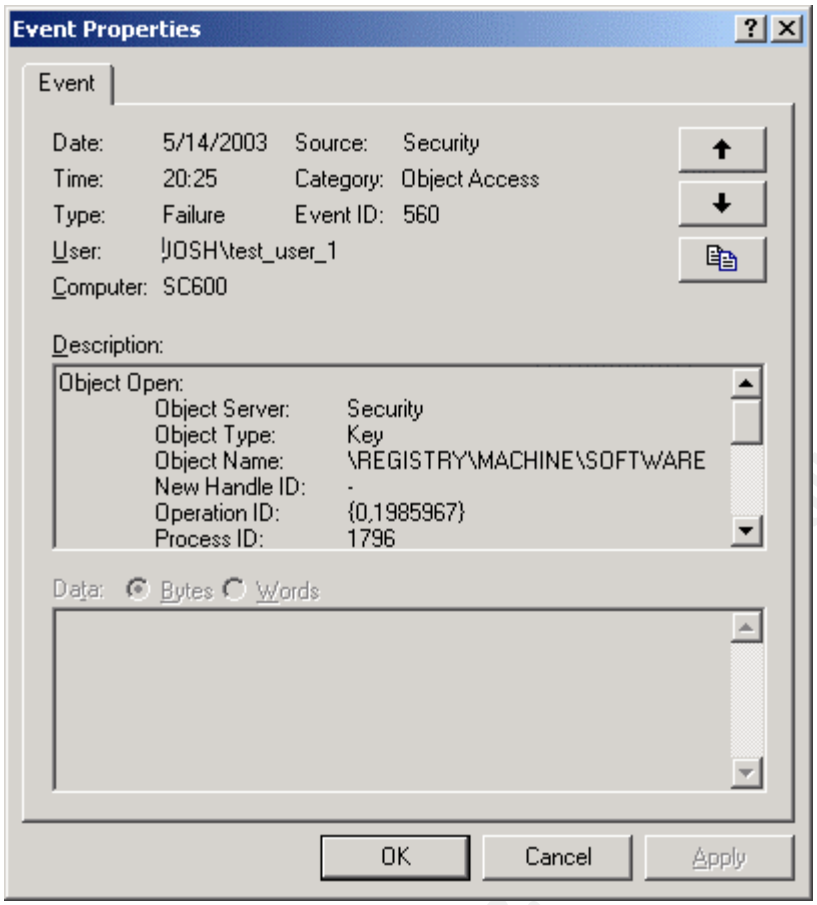
Test Analysis: Audit Object Access – Files and Folders

This test verified the "Audit object access" setting for files and folders. The user created a file and a folder and configured those objects to be audited by changing the SACL settings. The user then accessed the file and folder and edited the file. Checking the Security section of the Event Viewer revealed that success audits were not audited, as "Audit object access" is configured for only failure in the W2K-Server template. However, failure audits were recorded for the user's actions. Next the user removed the SACL settings and again accessed the file and folder and edited the file. Without the SACL set for the user, the failure events were not recorded in the Event viewer.

Test Procedures: Audit Object Access – Registry Keys

1. Launch the Registry Editor.
    a. Click Start | Run
    b. Type 'regedit' in the Run window
    c. Click OK
2. Drill down to the registry hive into the SOFTWARE section under HKEY_LOCAL_MACHINE.
    a. Expand HKEY_LOCAL_MACHINE | SOFTWARE
3. Enter the security properties of Software and grant Test_User_1 Read access.
    a. Click Add Button
    b. Scroll down and Click Test_User_1
    c. Click the Read check box only
4. Enter the audit properties of Software 1 and Audit Test User1
    a. Click Permissions from the Security menu
    b. Click the Security tab
    c. Click the Advanced Features pushbutton
    d. Click the Add pushbutton
    e. Scroll down and Click Test_User_1
    f. Click OK

5. Choose to audit Test_User_1 for Success for Set Value and Success and Failure for Create Sub-key.
    a. Click the Success check box for Set Value.
    b. Click the Success and Failure check boxes for Create Sub-key
    c. Click the Apply onto child objects checkbox
6. Log off of the Server.
    a. Click Start | Shutdown
    b. Choose Log off
    c. Click OK
7. Log on Test_User_1.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Test_User_1
    c. Enter the password
8. Launch the Registry Editor.
    a. Click Start | Run
    b. Type 'regedit' in the Run window
    c. Click OK
9. Drill down to the registry hive into the SOFTWARE section under HKEY_LOCAL_MACHINE.
    a. Expand HKEY_LOCAL_MACHINE | SOFTWARE
    b. Create a new key. This will fail with "Access Denied."
10. Log off of the Server.
    a. Click Start | Shutdown
    b. Choose Log Off
    c. Click OK
11. Log on as Administrator.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Administrator
    c. Enter the password
    d. Click OK
12. Log on a Server, open the Microsoft Management Console.
    a. Click Start | Run
    b. Type mmc in the Run window
    c. Click OK.
13. Add the Event Viewer Snap-in
    a. Click Console | Add/Remove Snap-in
    b. Click Add
    c. Choose Event Viewer
    d. Click OK
    e. Accept the default Local Computer by clicking Finish
    f. Click OK.
14. Check the Event Security Logs and confirm that registry key events were recorded properly.
    a. Verify a Failure Audit exists for accessing the Software registry hive



15. Launch the Registry Editor.
    a. Click Start | Run
    b. Type 'regedit' in the Run window
    c. Click OK
16. Drill down to the registry hive into the SOFTWARE section under HKEY_LOCAL_MACHINE.
    a. Expand HKEY_LOCAL_MACHINE | SOFTWARE.
17. Enter the audit properties of AuditFolder.
    a. Click Permissions from the Security menu
    b. Click the Security tab
    c. Click the Advanced Features pushbutton
18. Remove Test_User_1
    a. Scroll down and Click Test_User_1
    b. Click the Remove Pushbutton
    c. Click OK
19. Log off of the Server.
    a. Click Start | Shutdown
    b. Choose Log off
    c. Click OK
20. Log on Test_User_1.
    a. Press Ctrl-Alt-Del to bring up the Login Window

b. Enter the Username Test_User_1
c. Enter the password

21. Launch the Registry Editor.
    a. Click Start | Run
    b. Type 'regedit' in the Run window
    c. Click OK
22. Drill down to the registry hive into the SOFTWARE section under HKEY_LOCAL_MACHINE.
23. Expand HKEY_LOCAL_MACHINE | SOFTWARE. Attempt to create a new Key
    a. Right-click Software
    b. Click New | Key from the drop-down menu
    c. This will fail.
24. Log off of the Server.
    a. Click Start | Shutdown
    b. Choose Log Off
    c. Click OK
25. Log on as Administrator.
    a. Press Ctrl-Alt-Del to bring up the Login Window
    b. Enter the Username Administrator
    c. Enter the password
    d. Click OK
26. Log on a Server, open the Microsoft Management Console.
    a. Click Start | Run
    b. Type mmc in the Run window
    c. Click OK.
    d. Log on using a correct password.
    e. Click Console | Add/Remove Snap-in
    f. Click Add
    g. Choose Event Viewer
    h. Click Add
    i. Accept the default Local Computer by clicking Finish
    j. Click OK.
27. Check the Event Security Logs and confirm that registry key events were not recorded as auditing was turned off.
    a. Verify no audits exist for registry key events.
    b. Click OK after viewing each audit.

Test Analysis: Audit Object Access – Registry Keys

This test verified the "Audit object access" setting for registry keys. The user was granted only read access to the key hive and the hive was audited by changing the SACL settings. The user then accessed the registry key and attempted to create a key. Checking the Security section of the Event Viewer revealed that the failure audits were recorded for the user's actions. Next the user removed the SACL settings and again accessed the registry and attempted to create a

key. Without the SACL set for the user, the events were not recorded in the Event viewer.

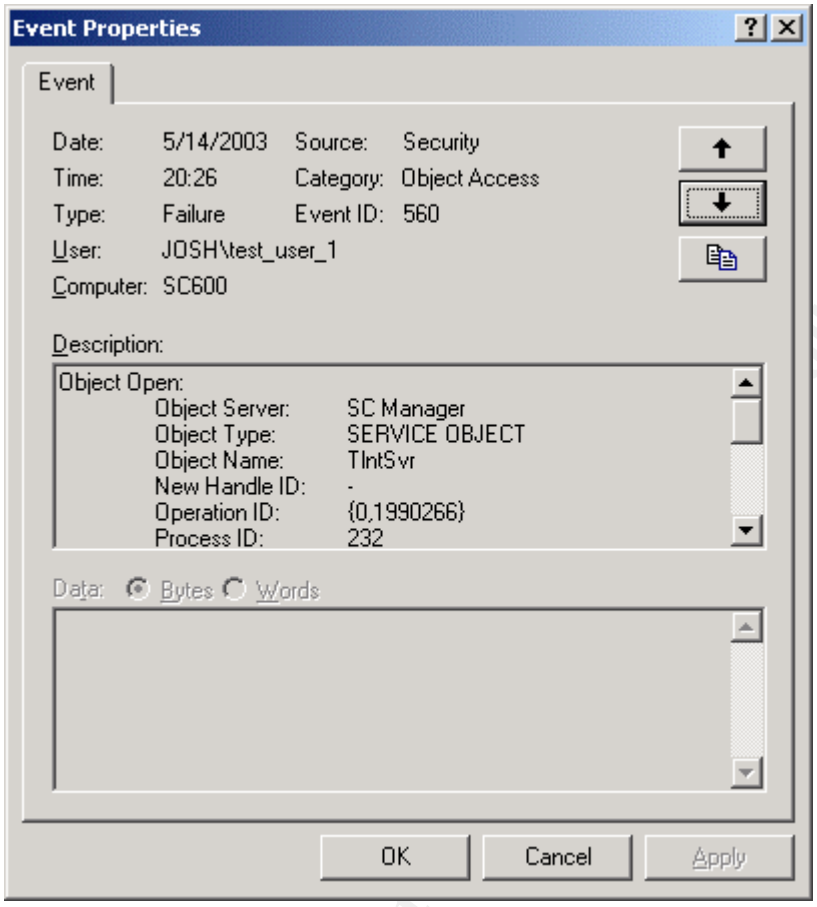
Test Procedures: Audit Object Access – Services

1. On a Server, open the Microsoft Management Console.
    a) Click Start | Run
    b) Type mmc in the Run window
    c) Click OK
2. Add the Group Policy Snap-In
    a) Click Console | Add/Remove Snap-in
    b) Click Add
    c) Choose Group Policy
    d) Click Add
    e) Click Close
    f) Click OK
3. Enter the audit properties of Telnet.
    a) On the OU Group policy, Drill down to Security Settings, System Services
    b) Double-click on Telnet.
    c) Click the 'Define this Security Setting' check box,
    d) Add Test_User_1 and click Deny for Full Control access
    e) Click the Advanced pushbutton
    f) Click on the Auditing tab
4. Add Test_User_1
    a) Click the Add pushbutton
    b) Scroll down and Click Test_User_1
    c) Click OK
5. Choose to audit Test_User_1 for Success for Start and Stop.
    a) Click the Failure check boxes for Start
    b) Click the Failure check boxes for Stop
6. Log off of the Server.
    a) Click Start | Shutdown
    b) Choose Log off
    c) Click OK
7. Log on Test_User_1.
    a) Press Ctrl-Alt-Del to bring up the Login Window
    b) Enter the Username Test_User_1
    c) Enter the password
8. Open the Microsoft Management Console.
    a) Click Start | Run
    b) Type mmc in the Run window
    c) Click OK
9. Add the Services Policy Snap-In
    a) Click Console | Add/Remove Snap-in

b) Click Add
c) Choose Services
d) Click Add
e) Click Close
f) Click OK

10. Attempt to Start the Telnet Service
    a) Right-click on the Telnet Service
    b) Click Start from the drop-down box
    c) An “access is denied” error is received
11. Log off of the Server.
    a) Click Start | Shutdown
    b) Choose Log Off
    c) Click OK
12. Log on as Administrator.
    a) Press Ctrl-Alt-Del to bring up the Login Window
    b) Enter the Username Administrator
    c) Enter the password
    d) Click OK
13. Log on a Server, open the Microsoft Management Console.
    a) Click Start | Run
    b) Type mmc in the Run window
    c) Click OK.
14. Add the Event Viewer Snap-in
    a) Click Console | Add/Remove Snap-in
    b) Click Add
    c) Choose Event Viewer
    d) Click OK
    e) Accept the default Local Computer by clicking Finish
    f) Click OK.

15. Check the Event Security Logs and confirm that registry key events were recorded properly.
    a) Verify a Failure Audit exists for Start from starting Telnet.



16. On a Server, open the Microsoft Management Console.
    a) Click Start | Run
    b) Type mmc in the Run window
    c) Click OK
17. Add the Group Policy Snap-In
    a) Click Console | Add/Remove Snap-in
    b) Click Add
    c) Choose Security Template
    d) Click Add
    e) Click Close
    f) Click OK
18. Enter the audit properties of Telnet.
    a) On the OU Group policy, Drill down to Security Settings, System Services
    b) Double-click on Telnet
    c) Click the Security option from the drop-down box.
    d) Click the 'Define this Policy check box

e) Click Edit Security
f) Click the Advanced pushbutton
g) Click on the Auditing tab

19. Remove Test_User_1
    a) Highlight Test_User_1
    b) Click Remove
    c) Click OK
20. Log off of the Server.
    a) Click Start | Shutdown
    b) Choose Log Off
    c) Click OK
21. Log on Test_User_1.
    d) Press Ctrl-Alt-Del to bring up the Login Window
    e) Enter the Username Test_User_1
    f) Enter the password
22. Open the Microsoft Management Console.
    d) Click Start | Run
    e) Type mmc in the Run window
    f) Click OK
23. Add the Services Policy Snap-In
    g) Click Console | Add/Remove Snap-in
    h) Click Add
    i) Choose Services
    j) Click Add
    k) Click Close
    l) Click OK
24. Attempt to Start the Telnet Service
    d) Right-click on the Telnet Service
    e) Click Start from the drop-down box
    f) An “access is denied” error is received
25. Log off of the Server.
    d) Click Start | Shutdown
    e) Choose Log Off
    f) Click OK
26. Log on as Administrator.
    a) Press Ctrl-Alt-Del to bring up the Login Window
    b) Enter the Username Administrator
    c) Enter the password
    d) Click OK
27. Log on a Server, open the Microsoft Management Console.
    a) Click Start | Run
    b) Type mmc in the Run window
    c) Click OK.
    d) Log on using a correct password.
    e) Click Console | Add/Remove Snap-in
    f) Click Add

g) Choose Event Viewer
h) Click Add
i) Accept the default Local Computer by clicking Finish
j) Click OK.

28. Check the Event Security Logs and confirm that audits for services were not recorded as auditing was turned off.

a) Verify no audits exist for services events
b) Click OK after viewing each audit

Test Analysis: Audit Object Access – Services

This test verified the "Audit object access" setting for services. The administrator configured a service to be audited by changing the SACL settings. The Telnet Service was configured to deny access to the test user. The test user then attempted to start the Telnet. Checking the Security section of the Event Viewer revealed that failure audits were recorded for the test user's actions. Next the user removed the SACL settings and again attempted to start the service. Without the SACL set for the user, the events were not recorded in the Event viewer.

TESTING THE SYSTEM'S FUNCTIONALITY

This section will test the expected functionality of system with the Security Template applied. This will demonstrate whether the template can be applied without any changes or if different configurations will be necessary to allow end-users or support personnel to complete normal everyday tasks.

The tests covered here will focus on access the support team will need to the production server. Under the company's Windows 2000 security policy, server support personnel access will follow a least privileged security model. While Administrator access to a server might be an easy fix for providing the support group the rights they require, it would clearly give them more rights than necessary and not adhere to the least privileged security model.

The first test will cover access to log on to the Windows 2000 application server using Terminal Services client software. The proprietary database on the server has a database performance and maintenance tools available only on the server itself. The vendor of the software offers neither a client version of the tools to allow remote connections to the database, nor does the vendor provide an Microsoft Management Console snap-in for the tools. Therefore, the support group must be able to log onto the server to complete their duties, but company policy will prevent them from having access to the computer console. They will need Terminal Services access.

The second test will cover access to the Application logs within the Event Viewer on the Windows 2000 Server. The support personnel monitor the Event Viewer to monitor the health of the application and to aid in troubleshooting possible application issues.

The third test will cover FTP access to the Server. The application requires FTP updates from a mainframe every evening. An FTP account will be set up within the Windows 2000 environment. This account will require read and write access to the C:\FTPDATA directory.

Test 1: Terminal Services Access

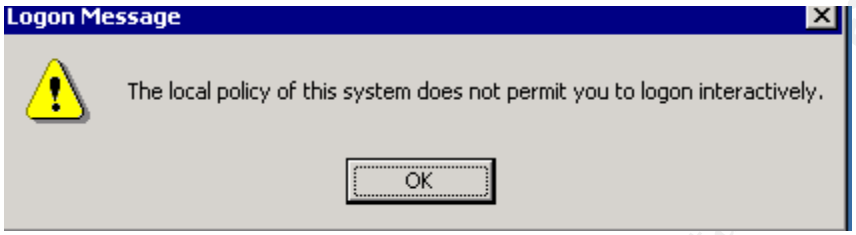
Test Procedures: Terminal Services

Assumed: Terminal Services Server has been installed on the Server.

1. Log on a Windows 2000 Workstation, open the Microsoft Management Console.
    b) Click Start | Program Files | Administrative Tools | Terminal Services Client
    c) Click the Terminal Services Client Application

d) The Terminal Services Client opens

2. Connect to the Server
    a) Type the Server Name
    b) Click Connect
    c) Type proper Support Account Username and Password for a user in the application support group (OPTION_SUP_GRP)
    d) Click OK
    e) The log on fails with the following error: "The local policy of this system does not permit you to logon interactively"



3. Continue testing after configuring the application support group (OPTION_SUP_GRP) to have logon locally rights under Security Settings\Local Policies\User Rights Assignment\Log On Locally
    a) Click Start | Program Files | Administrative Tools | Terminal Services Client
    b) Click the Terminal Services Client Application.
    c) The Terminal Services Client opens.
4. Connect to the Server
    a) Type the Server Name
    b) Click Connect
    c) Type proper Support Account Username and Password for a user in the application support group (OPTION_SUP_GRP)
    d) The log on fails with the following error: "You do not have access to this Session".

Test Analysis: Terminal Services Access

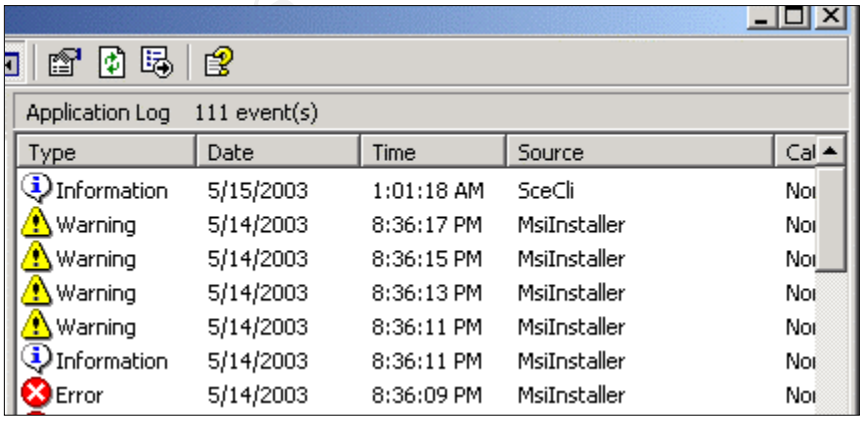
This test entailed logging onto the server using Terminal Services Client as a member of the application's support group. The first time this failed with the "The local policy of this system does not permit you to logon interactively" error. According to Microsoft, "the user attempting to log on does not have the "logon locally " permission available under Security Settings\Local Policies\User Rights Assignment\Log On Locally." The NSA's template configures this policy for Administrators only. However, for the application support group, OPTION_SUP_GRP, to have access to Terminal Services on the server, they need to be added as well. Once the group was configured to have "Logon

locally" rights within group policy, the test was tried a second time. This failed with the "You do not have access to this Session" error. According to Microsoft, "The user attempting to log on does not have sufficient permissions on the appropriate RDP-TCP connection." This can only be corrected by using Terminal Services Configuration to grant the application group the logon permission. This is not possible in Windows 2000 through the Security Template or group policy.

Test 2: Event Viewer Access

Test Procedures: Event Viewer

1. Log on a Windows 2000 Workstation as a member of the Application Support Group, open the Microsoft Management Console.
    a) Click Start | Run
    b) Type mmc in the Run window
    c) Click OK.
    d) Click Console | Add/Remove Snap-in
    e) Click Add
    f) Choose Event Viewer
    g) Click Add
    h) Click the Another Computer radio button
    i) Type in the name of the Server
    j) Click Finish
    k) Click Close
    l) Click OK.
2. Open the Application section of the Event Viewer
    a) Expand the Event Viewer tree
    b) Click on Application
    c) The Application section appears successfully
    d) Click File
    e) Choose Exit



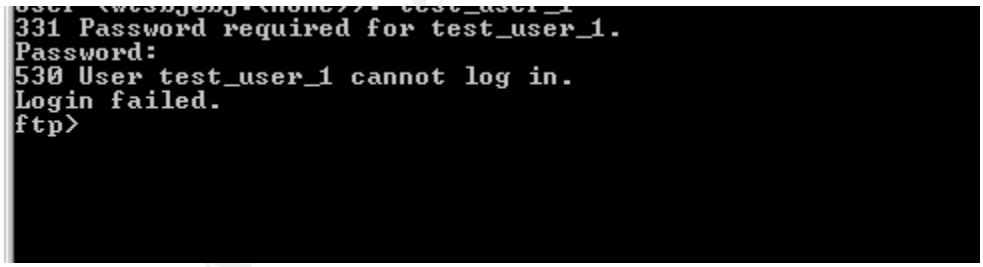
Test Analysis: Event Viewer

This test involved determining whether the support group would be able to access the Application logs within the Event Viewer on their Windows 2000 Server. This entailed logging on to a workstation as a member of the Application Support Global Group, connecting to the server's Event Viewer using the MMC, then viewing the Application logs. This test was successful. Unlike the first test, the W2K_Server template was not too restrictive in this case.

Test 3: FTP Access

Test Procedures: FTP Access

1. Log on a Windows 2000 Workstation, open the command prompt.
    a) Click Start | Run
    b) Type cmd in the Run window
    c) Click OK.
2. FTP to the server using a preconfigured FTP account name and password
    a) Type FTP 192.168.123.115 (server name)
    b) Hit Enter
    c) Type the FTP account name (Test_User_1) for user.
    d) Hit Enter
    e) Type the appropriate password for the account
    f) Hit Enter
    g) The FTP login fails



Test Analysis: FTP Access

This test involved connecting to the server with Test_User_1, a dedicated FTP account. This account was already granted read and write access to the virtual directory to which it required access. However, the test failed because the Test_User_1 account did not have logon locally rights to the server. The W2K_Server Template configures "Logon locally" for Administrators only. This right (to logon locally) is required for anyone trying to connect to the FTP server, because this right is used by the FTP Service to allow the connection (SOURCE). Therefore, the Test_User_1 account itself, or a group it belongs to,

must be added to have the “Logon locally” right in order to successfully connect to the server.

TEMPLATE EVALUATION

As the tests clearly demonstrated, there were certainly areas where the template proved to be too strong for the application. The support group requires "logon locally" access to enable them to connect to the server using the Terminal Services client. The W2K_Server Template defines "logon locally" for Administrators only. Adding the support group to the Administrators group would violate the company's least privileged security model. The support group would have to be added to the "logon locally" policy to accommodate Terminal Services access.

Similarly, this same issue would adversely affect the functionality of the application itself since it requires the delivery of data over FTP from a mainframe. Accounts cannot access directories on the server over FTP without being granted "logon locally" rights. Since the W2K_Server Template defines "logon locally" only for Administrators, the FTP account would have to be added to the "logon locally" policy to allow the application to function properly.

However, these template shortcomings are due to special circumstances for this application, they are not limitations that would affect all application servers. There would certainly be applications that could operate effectively under this template, but there are unquestionably others that would require adjustments in other policy areas to operate effectively.

This is not to say that the template should be altered to be more compatible with the many different requirements across different servers. Microsoft has taken criticism for setting up Windows 2000 defaults with such lax security configurations. Windows 2000 defaults force those looking to secure their servers to lock down the exposed security vulnerabilities themselves as opposed to having it locked down by default. The risk to server security is much higher when a burden exists to identify the various security risks and lock those down, rather than having to instead identify what areas are secured too tightly and then open those areas up. In other words, an open environment that requires securing comes with higher risks than a closed environment that requires opening up. The security risks that are reduced with a closed default environment outweigh the gains in functionality with the open security environment.

Outside of specific requirements for this application, there are various changes that would need to be made for this template to function properly in the company's environment as a whole. Here are some of the changes that would be required:

- The "Backup files and directories" setting is configured for Administrators only within the "W2K_Security" Template. As the company makes use of the Backup Operators group, the Backup Operators group must be added

to this policy to enable the group to be permitted to back up directories and files.

- The "Debug programs" setting is defined for no one under the NSA's template. Certain company developers temporarily require this right to debug low-level objects. Rather than adjust group policy each time the developers require this access, a group that the developer would be temporarily added to would be configured within the "Debug programs" setting.
- Various applications within the environment have services that require the "Logon as a service" right. The "W2K_Security" Template defines this setting for no one. "Logon as a service" would need to be configured for the necessary services.

Of course, there is a trade-off to altering the locked down settings of the NSA's template. Although it allows certain system-specific security requirements to be met, it does open up risks in other areas. For instance, since FTP passes its username and password in clear text, there is a clear risk that the username and password could fall into the wrong hands. Since this FTP account is being granted "log on locally" access, the person that gains access to the username/password combination would also gain local logon capability to the server. Additionally, if someone discovered the password to a service account with "logon as a service" rights, that person could use that access in damaging ways. Further research could be done to investigate the auditing of FTP and Service accounts on the Windows 2000 network. The care given in keeping the passwords to these accounts secret and out of hands of support and end-users would also go far into accounting for the risk involved in opening up areas of the "W2K_Server" Template.

Although the NSA's Template went far to lock the server down, there are still areas where it could go even further. In particular, the Services policies were left undefined. Unused services would be better off configured as disabled. For example, services such as Telnet, Terminal Services, and FTP would lower security risks if defined as "disabled" within the template. They could then be configured if necessary for systems to which the template is applied. The NSA could have gone through and left all non-critical services disabled within its template.

While Windows 2000 Security Templates and other Group Policy tools are a major improvement over what was provided within the Windows NT environment, there are still areas that could be approved upon. For instance, when a Security Template is applied at the domain level and within different OU levels, it can be difficult to figure out what specific settings are applied to individual system. Windows 2000 does not provide a tool that will define the resultant set of policies for a certain user on a specific system. There are tools that can be purchased to provide such functionality, such as FAZAM 2000, but this type of tool will not be available from Microsoft until Windows Server 2003. Additionally, the ability to do

"what if" scenarios with applying multiple templates to different domain, site, and OU levels ant the ability to audit changes in Group Policy would also make the management of multiple systems in an enterprise environment more efficient.

APPENDIX A: W2K_Server Registry Settings

Registry Key	Groups	Template Permissions	Inherit Method
CLASSES_ROOT\	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys) Full Control Read	Replace
\MACHINE\SOFTWARE	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys) Full Control Read	Replace
\MACHINE\SOFTWARE\Microsoft\NetDDE	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SOFTWARE\Microsoft\ OS/2 Subsystem for NT	Administrators CREATOR OWNER SYSTEM	Full Control Full Control (Subkeys only) Full Control	Replace
\MACHINE\SOFTWARE\Microsoft\ Protected Storage System Provider			Ignore
\MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\AsrCommands	Administrators Backup Operators CREATOR OWNER SYSTEM Users	Full Control Query, Set Value, Create Subkey, Enumerate, Notify, Delete, Read permissions Full Control (Subkeys only) Full Control Read	Replace
\MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\Perflib	Administrators INTERACTIVE CREATOR OWNER SYSTEM	Full Control Read Full Control (Subkeys only) Full Control	Replace
\MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Group Policy	Administrators Authenticated Users SYSTEM	Full Control Read Full Control	Propagate
\MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Installer	Administrators SYSTEM Users	Full Control Full Control Read	Propagate
\MACHINE\SOFTWARE\Microsoft\Windows \ CurrentVersion\Policies	Administrators Authenticated Users SYSTEM	Full Control Read Full Control	Propagate
\MACHINE\SYSTEM	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Replace
\MACHINE\SYSTEM\clone			Ignore
\MACHINE\SYSTEM\controlset001	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset002	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset003	Administrators CREATOR OWNER	Full Control Full Control (Subkeys only)	Propagate

	SYSTEM Users	Full Control Read	
\MACHINE\SYSTEM\controlset004	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset005	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset006	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset007	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset008	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset009	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset010	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg	Administrators Backup Operators SYSTEM	Full Control Read (Key only) Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Control\Wmi\Security	Administrators CREATOR OWNER SYSTEM	Full Control Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Enum			Ignore
\MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers	Administrators CREATOR OWNER SYSTEM	Full Control Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities	Administrators CREATOR OWNER SYSTEM	Full Control Full Control Full Control	Replace
USERS\.DEFAULT	Administrators Users CREATOR OWNER SYSTEM	Full Control Read Full Control (Subkeys only) Full Control	Replace

USERS\.DEFAULT\Software\Microsoft\ NetDDE	Administrators SYSTEM	Full Control Full Control	Replace
USERS\.DEFAULT\Software\Microsoft\ Protected Storage Systems Provider			Ignore

APPENDIX B: W2K_Server File System Settings

Folder/File	Groups	Template Permissions	Inherit Method
%ProgramFiles%	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Replace
%ProgramFiles%\Resource Kit	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Replace
%SystemDirectory%\appmgmt	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate
%SystemDirectory%\config	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\dllcache	Administrators CREATOR OWNER SYSTEM	Full Control Full Control Full Control	Replace
%SystemDirectory%\DTCLog	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Propagate
%SystemDirectory%\GroupPolicy	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control	Propagate
%SystemDirectory%\ias	Administrators CREATOR OWNER SYSTEM	Full Control Full Control Full Control	Replace
%SystemDirectory%\Ntbackup.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\NTMSData	Administrators SYSTEM	Full Control Full Control	Propagate
%SystemDirectory%\rcp.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\Regedt32.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\ReinstallBackups			Ignore
%SystemDirectory%\repl	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate
%SystemDirectory%\repl\export	Administrators Replicator SYSTEM Users	Full Control Read, Execute Full Control Read, Execute	Propagate
%SystemDirectory%\repl\import	Administrators Replicator SYSTEM Users	Full Control Modify Full Control Read, Execute	Propagate
%SystemDirectory%\rexec.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\rsh.exe	Administrators SYSTEM	Full Control Full Control	Replace

%SystemDirectory%\secedit.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\Setup	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\spool\Printers	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Traverse folder, Read attributes, Read extended attributes, Create files, Create folders (folder and subfolders)	Replace
%SystemDrive%	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Propagate
%SystemDrive%\autoexec.bat c:\autoexec.bat	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%SystemDrive%\boot.ini c:\boot.ini	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\config.sys c:\config.sys	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%SystemDrive%\Documents and Settings	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate
%SystemDrive%\Documents and Settings\Administrator	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\Documents and Settings\All Users	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate
%SystemDrive%\Documents and Settings\Default User	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%SystemDrive%\Documents and Settings\ All Users\Documents\DrWatson	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Traverse folder, Create files, Create folders (subfolders and files) Read, Execute	Replace
%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson\drwtsn32.log	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control Full Control Modify	Replace
%SystemDrive%\Inetpub			Ignore
%SystemDrive%\io.sys	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%SystemDrive%\msdos.sys	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%SystemDrive%\My Download Files	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Write, Execute	Replace
%SystemDrive%\ntdetect.com c:\ntdetect.com	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\ntldr c:\ntldr	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\System Volume Information			Ignore

%SystemDrive%\Temp	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Traverse folder, Create files, Create folders (subfolders and files)	Replace
%SystemRoot%	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Replace
%SystemRoot%\$NtServicePackUninstall$	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\$NtUninstall* (all uninstall folders)	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\CSC	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\debug	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Replace
%SystemRoot%\debug\UserMode	Administrators SYSTEM Users	Full Control Full Control Traverse folder, List folder, Create files (folder only)	Propagate
%SystemRoot%\security	Administrators CREATOR OWNER SYSTEM	Full Control Full Control (subfolders and files) Full Control	Replace
%SystemRoot%\Offline Web Pages			Ignore
%SystemRoot%\regedit.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\Registration	Administrators SYSTEM Users	Full Control Full Control Read	Propagate
%SystemRoot%\repair	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\Tasks			Ignore
%SystemRoot%\Temp	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Traverse folder, Create files, Create folders (folders and subfolders)	Replace
C:\ntbootdd.sys	Administrators SYSTEM	Full Control Full Control	Replace

REFERENCES

"Error Messages Generated When Logging on with Terminal Services Client." Microsoft Knowledge Base Article – 246109. 10 Oct 2002. http://support.microsoft.com/?kbid=246109 (18 April 2003).

Haney, J. Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set. Ft. Meade: National Security Agency. 2002.

Harris, Shon. All In One CISSP Certification Exam Guide. Berkeley:McGraw-Hill/Osborne, 2002. 238.

Microsoft Windows 2000 Security Technical Reference. Redmond:Microsoft Press. 2000.

Your Domain Users receive Event ID 100, 'Access Denied', when attempting to FTP to Windows 2000 IIS? 3339. http://www.jsifaq.com/SUBG/TIP3300/rh3339.htm (20 April 2003)

Last Updated: September 19th, 2017

Upcoming Training

Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
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 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**