Global Information Assurance Certification Paper

GIAC Windows Security Practical

Option 2

Securing Windows 2000 with Security Templates Ver. 3.1 (revised April 8, 2002)

Prepared by: Sean C. Speegle
Date: 2-5-2002

TABLE OF CONTENTS

DESCRIPTION ... 3

Checklist or Template ... 6

Security Settings ... 6

Account Policies ... *8*

Lockout policy ... *9*

Kerberos Policy ... *9*

Audit Policy ... *9*

User Rights Assignment ... *10*

Security Options ... *10*
Clear the Virtual page file when shutting down ... 10
Message text for users logging on ... 10
Rename the administrator account ... 10
Shut down system immediately if unable to log security audits ... 11

Settings for Event Logs ... *11*

Maximum application log size ... *11*

Restrict guest access to application log ... *11*

Restrict guest access to security log ... *11*

Restrict guest access to system log ... *11*

Retain application log ... *11*

Retain security log ... *11*

Retain system log ... *11*

System Services ... 12

Alerter ... *12*

Automatic Updates ... *12*

Clip book ... *13*

Fax service ... *13*

Indexing service ... *13*

License Logging service ... *13*

Messenger ... *13*

NT LM Security Support provider ... *13*

Remote Access Auto connection manager ... *13*

Routing and remote access ... *13*

Telephony ... *13*

Telnet ... *13*

Enhanced file security 15

Apply the Template 17

Critical File Security 21

Disabled Services *23*

Test the system functionality 24

Log on as administrator *25*

Evaluate the template 32

Appendix A: 33

Appendix B: 49

Appendix C: 52

DESCRIPTION

Standard file servers play an important role in a network environment. They need to be configured to allow all authorized users access to shared resources while maintaining strict access control to areas of the server that are not authorized like making configuration changes that can affect the operation of the server. Depending on the environment you may have. For example: Junior administrators may need to logon to the server to do their jobs but do not yet have all the skills needed to be given complete control over the server. Senior administrators still need to maintain administrative control over all servers in the domain and users still need to connect, print and save files to the server while doing their jobs. These resources need to be protected by correctly securing the file server.

Configuring these systems used to require system administrators to follow a published "checklist" of settings (from Microsoft or third party vendors) and to manually go through the list to properly secure the system prior to putting it on the wire and making the system available to users. System administrators would then need to manually re-check the systems every so often to make sure that the correct settings were still in force on each system. This would take a considerable amount of time on just a few systems, much less the burden placed on system administrators maintaining hundreds of systems.

Microsoft has addressed this issue with the development of the security configuration manager, security templates and Active Directory. With the security configuration tool, administrators can develop security templates that make all of the required security settings to systems based on their roles in the environment, file servers; domain controllers; web servers etc. all need different and specialized configurations to become secure. Once a template has been configured to secure the system properly, it can be used on any system that requires the same settings and can

configure the system in minutes rather than the hours it used to take to manually configure the same types of systems with old NT. Once in place, the settings are automatically "refreshed" to insure that the settings aren't changed from the original configuration. Also, the security configuration manager can be used to audit the settings of servers anytime by doing an analysis of the system based on the original template that was used to configure the system. The original template is a benchmark of the final configuration. This way, administrators can be certain that the settings that were in place when the system was configured are still in place and have not changed. Changes could indicate that the system has been compromised or possibly reconfigured by a well meaning junior admin. If the settings have changed from the original configuration then further investigation is required.

The following scenario is a hypothetical. Any Town Bank does not exist as a real company. Active Directory was setup in a test environment to describe and illustrate how to apply security templates for a Windows 2000 server in a domain environment at a branch office setting. Any similarities to any known or unknown companies are purely coincidental. As always, be sure to test all of the settings described here before deploying to production equipment.

Any Town Bank has a branch office located in a suburb of Any Town, USA. It is a small office that has 12 employees. Job descriptions include; 3 loan officers, 7 Bank tellers, plus a branch manager and a receptionist. A single file server will be located at the branch to manage the local file shares where branch employees save their work. The system will also be a DHCP server to hand out IP address for the local office, plus house the "home drives" for local users at the branch. The branch is connected to the "home office" via 2 T1 links for redundancy. For security reasons Any Town bank does not allow remote DC's at any branch office so Logon authentication and any enterprise mainframe applications will be hosted from the home office via this link.

The hardware for the system consists of a Dual 900 MHz P-III Compaq Proliant DL 380 server with 640 MB RAM, Dual power supplies, (2) 9.1 GB and (3) 36.4 GB hard drives configured via Compaq hardware RAID controller as 2 logical drives. The two 9.1 GB drives will be mirrored to house the operating system; the three 36.4 GB drives will be configured as a RAID 5 set for data storage. Redundant power supplies ensure uninterrupted operation of the server should one of the power supplies fail. An APC 2200 Battery backup is connected in case of power outages the server will be able to run for a brief period then is configured to automatically shutdown if the power outage is longer than 10 minutes. All of these precautions; fault tolerant disk sets, power supplies, and UPS battery backup should minimize any downtime as both the power supplies and the hard drives are all hot swappable. During normal server operation, there is no need to power off the server to complete the repairs.

As a best practice, the file server was loaded on a clean hard drive with Windows 2000 Server while *disconnected* from the network. This will ensure that in no way can this system be compromised during the installation phase. The file system was

formatted with NTFS for file security, Windows 2000 Service pack 3 and post service pack security hot fixes were applied to the system prior to connecting the server to the network from CD-ROM. All of the hotfixes that were available at the time this server was being configured were downloaded from Microsoft's TechNet security website then burned to CD, then installed in order. Once the OS was configured and patched, anti-virus software was installed. Symantec Corporate anti-virus version 7.6 was chosen because it monitors all files that are saved to, and copied from the server in real-time, preventing any virus from infecting the server or spreading any viruses to other workstations in the domain. The propagation of "share aware" viruses like Klez could allow improperly configured network shares to be vectors of infection to users of the system / Domain. Since this server houses users Home Drives, the scanning of all files inbound and outbound from the server will eliminate the possibility for users to store and unknowingly propagate viruses to other users. The virus definitions will be updated automatically from the home office, this way, the system will not need to connect to the internet for its virus definition updates. This also allows for quick updates to be rolled out quickly from a known central location in case of a new virus outbreak. In addition to "real-time" file scanning, the anti-virus software has been configured to do a nightly scan of all files on the system during off hours and to quarantine any files that it finds to be infected. Quarantining the files instead of deleting was chosen so that false positives would not delete critical files or documentation, even though moving the files to a quarantined directory may still break some function of the server, this file can be quickly copied back into place provided that it is deemed safe and was just a false positive.

This server will be configured to be a file / print server only and will not host any Enterprise applications. Its primary purpose will be to provide an area for users to save personal files, manage and offer access to the local office printers and act as a DHCP server to hand out IP addresses to workstations at the branch. Also, a "common" shared file area for locating and accessing the Branch offices policies and procedures documentation, signature cards etc. should also be accessible to all workstations. End users will be using this server to print to the office printers and connect to their "home drives" for storing their personal work files and documents. End User systems are identically configured Compaq DeskPro EN workstations loaded with Windows 2000 Professional, Intel® Pentium® III processor 733 MHz, 256 MB RAM, Integrated Intel Pro/100 VM NIC, 20GB/7200 rpm Smart III Ultra ATA 100 HDD cloned and configured by home office and shipped to the branch after configuration. Installations of the workstations are accomplished by regional technicians dispatched by home office when an order is completed.

The server will be located in a secured area of the office. This alarmed, air conditioned and locked room is not accessible to anyone except the Branch Manager. He/she will be the one person that will replace the nightly tape for that evening's backup of the system and any other routine maintenance. This is where all network switches and routers for the office are located. The locked door and strict access requirements should minimize any physical access to the server and network equipment. The system will be administered remotely from the "Home Office" using Microsoft's built-in terminal services configured for remote administration. The company has deployed Active Directory and this server will be located in the OU created for all Branch file servers in

the Active directory. Group policy will be used to enforce all security settings and will be applied at the OU level.

Checklist or Template

Microsoft has created several "pre-built" security templates that are installed to the *C:\winnt\security\templates* directory during installation. These templates have several different basic security designs pre-created by Microsoft. Although these templates are in and of themselves good basic starting points for creating a useful template, I have chosen the NSA w2k_server.inf security template as a baseline for this system. The reason I chose the NSA template over the Microsoft templates is because the NSA template already uses the Microsoft SecureDC.inf template as a starting point in its configuration, and is designed for file servers. The NSA template was also chosen because it is a consensus template created from the input of several government organizations and technical partners of the NSA. Because of this, it gives a broad scope of experience from different organizations for the templates initial settings. Microsoft is a single organization and is known for "loose" configurations mostly for backwards compatibility, (though they are now making strides to reverse this perception since Code Red) I feel that having the NSA and its partners review and document the settings from a consensus point of view greatly enhances and legitimizes the template. Most settings are already configured securely and this template should take minimal changes to configure it for this server's particular need and the security policies of the company. . The link for this template can be found at the NSA web site.
http://www.nsa.gov/snac/index.html

Security Settings

To view the security settings that are configured in the NSA server template, we will import the template into the security configuration editor so that we can make appropriate changes to the settings for our environment then export the new settings to a new file for our OU's security policy. We are securing the server as an OU group Policy and are not configuring any settings locally. Any local settings will be overwritten by the GPO from the parent OU in the Active Directory.

Now we will create our custom security template based on the NSA File server template that we chose for our configuration. First we need to save it to an appropriate directory. I chose to save the NSA template to the same directory where the Microsoft supplied security files are stored, under %systemroot%\security\templates as depicted in the screenshot. See Figure 1 below.

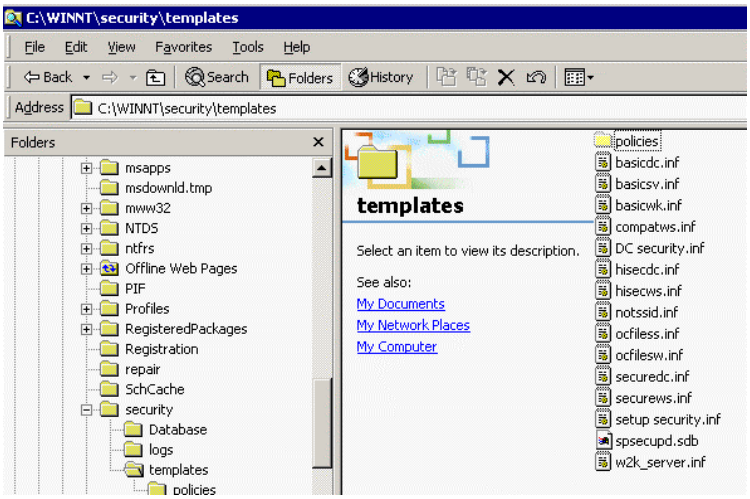


Figure 1

Then we open the MMC to add the Security templates snap-in to make the changes that we talked about above. (See Figure 2). Go to the start button and choose run. From the run line type mmc, this will open the mmc with no snap-ins added. Go to the console drop down menu and choose Add/Remove snap-in. Choose Security Templates and then close each open dialog box.

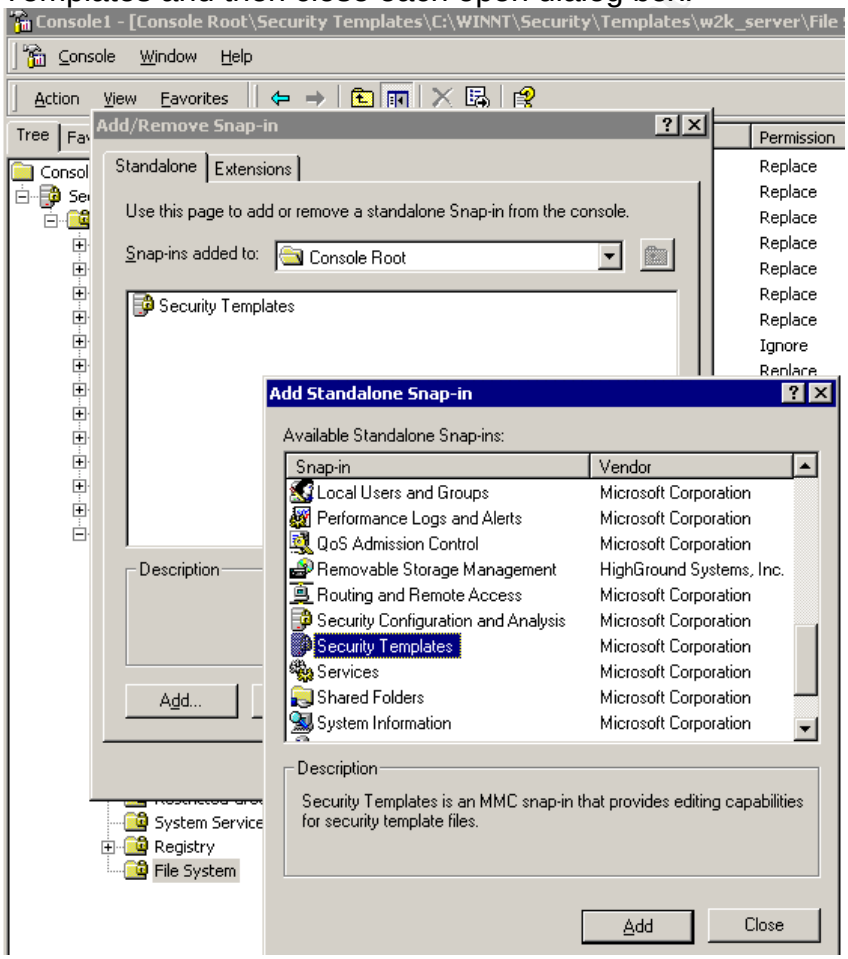


Figure 2

At this point you are presented with the security templates directory and all of the templates to choose from. We will be configuring, and then saving the NSA template called W2k_Server highlighted in the screenshot. See Figure 3 below.

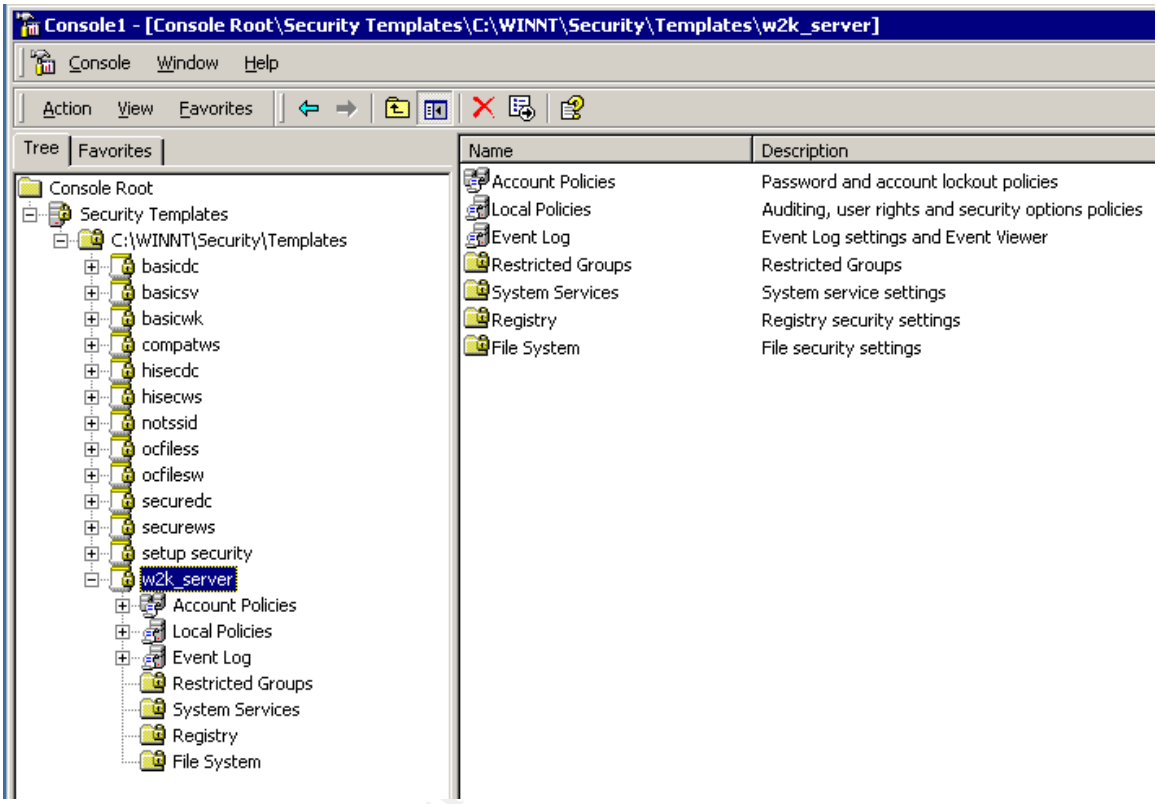


Figure 3

Account Policies

The first settings in the template are account policies for password lockout and Kerberos. These settings are applied at the domain level of the organization and therefore are not required to be processed by the server for this OU. We will change the template so that the password policy is not configured at this level. We will show later that the password policy is indeed processed by inheritance from the domain later in this document by trying to create passwords that do not comply with the Domain policy. **Note**: not defining the password policy locally was done to "illustrate" how the password policy was indeed inherited by the domain GPO. Though as a "best practice" it you should configure the local password policies to match what is set at the domain level. Kerberos policies are only configured at the domain level.
See Figure 4.

Policy	Computer Setting
Enforce password history	Not defined
Maximum password age	Not defined
Minimum password age	Not defined
Minimum password length	Not defined
Passwords must meet complexity requirements	Not defined
Store password using reversible encryption for all users in the domain	Not defined

Figure 4

Lockout policy

Policy	Computer Setting
Account lockout duration	Not defined
Account lockout threshold	Not defined
Reset account lockout counter after	Not defined

Figure 5

Kerberos Policy

Again, the Kerberos policy is configured at the domain level and will be applied when the server boots up.

Audit Policy

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

Figure 7

Most of the settings for auditing that the NSA has recommended are sufficient for this file server, a couple of changes will be made to these settings though. We will add success to “Audit privilege use” setting although we could have chosen to audit success on object access too, choosing failure only on object access is good for two reasons; 1) it will prevent excessive logging to the event logs and 2) will make it easier to catch failed actions. If successful logging on object access was also being audited, this tends to produce huge amounts of information and the log files would also be much larger and harder to manage. This could make it easier to miss failed attempts to access files as they could get lost in the “success” audits. See figure 7 above.

User Rights Assignment

The settings for User Rights are very secure as set by the NSA template. As configured it will only allow members of the Administrators group to logon locally, shutdown the server and do all of the management of the system. The other configuration that bears mentioning in this section, will only allow "administrators" and "users" network access to the server, which is the *"access this computer from the network"* right. Users will obviously need this access right in order to access the shared files that they store on the machine. Other than that, Administrators and branch managers are the only group allowed to logon locally; everyone else will be accessing this server from the network to connect to the proper shares or to print etc. We will also be adding the branch managers group to the "logon locally" right when we save the template so that people in the "branch managers" group can logon locally if needed. As a side note: "Domain Users" "Authenticated users" and "interactive users" are also members of the local "users" group by default. You cannot control the members of these "implicit" groups for example because any users that "authenticate" automatically become members of the authenticated users group except anonymous and any users that are logged on locally to the server become members of the "interactive" group, so controlling how the "users" group gets access to the server effectively limits access by these implicit groups as well.

Security Options

Here, most of the security options that NSA has recommended are going to be more than adequate. There are some settings that we will be changing to better fit into our environment. These changes are discussed below:

1. **Clear the Virtual page file when shutting down**: We will disable that setting as in this environment the server is in a physically secured area and the threat of getting information from the page file after shutdown is remote. The faster turn around time on reboots outweighs the minimal chance that any malicious user could access the page file after shutdown, this will improve shutdown / reboot time significantly.
2. **Message text for users logging on:** Create a warning and logon banner that warns users that all actions are being monitored to cover you legally. If you don't maintain a logon banner users could state that they did not know it wasn't a system for "authorized use only" Check with your lawyers for the wording if needed.
3. **Message Title for users attempting to log on:** The title for our logon message box will be Warning!
4. **Rename the administrator account**: This setting will be changed from the default of "not defined" This setting is used to make the administrator account more secure by renaming it from a known value. It is still possible to enumerate

the administrators account but just makes it more difficult to find. We will rename the Administrator account to LNTQ, you don't need to rename with another "name" you can use obscure words or random letters if you want. Don't forget to create a "fake" administrator account give it a secure password and disable it as a decoy.

5. **Rename guest account**: Same description as above. We will rename the guest account to zbod. To obscure the guest account name.
6. **Shut down system immediately if unable to log security audits:** This setting will shut the server down if the security logs fill up. This setting is too strict for our use and will be disabled as we will implement the automated clearing and saving of the event logs via an automated script. The use of this setting can also be used as a denial of service attack if a nefarious user can fill the security log then he can shut you down, so think twice before enabling this setting.

Settings for Event Logs

1. **Maximum application log size:** this setting specifies how big the application, system, and security log files can grow. This setting affects all security logs the same way. We will change this setting to a more reasonable setting during our configuration (approx.100MB) from the NSA defined setting of (4194240). We will be managing these logs with a script to archive the logs daily and 100MB is sufficient for the needs of the file server.
2. **Restrict guest access to application log**: This setting will not allow guest access to the application logs, i.e. you must authenticate to view the logs.
3. **Restrict guest access to security log**: This setting will not allow guest access to the security logs, i.e. you must authenticate to view the logs.
4. **Restrict guest access to system log:** This setting will not allow guest access to the system logs, i.e. you must authenticate to view the logs
5. **Retain application log:** this setting will not overwrite a log setting until it is the specified "days" old, in our case we will allow overwriting of the logs at 7 days.
6. **Retain security log**: this setting will not overwrite a log setting until it is the specified "days" old, in our case we will allow overwriting of the logs at 7 days.
7. **Retain system log**: again this setting will not overwrite a log setting until it is the specified "days" old, in our case we will allow overwriting of the logs at 7 days.

I think that the event logs are sized too big in the template which is the maximum allowed, and I will reduce the max log size to 100MB. This should be plenty of room to log the system events.

.

We will also implement a simple batch file that will archive and clear the logs on a daily basis so this will not present any problems. They will then be copied to a remote server for archiving and examination using the resource kit utility dumpel.

Restricted Groups

The restricted groups' container is empty by default on the NSA template, we will be adding the local administrators group and will restrict group membership to be only local the administrator account and the Domain Admins Global group. This will ensure that only authorized users will be members of this group.

System Services

All servers and their environments are not alike. Web servers, file servers and Domain Controllers all require specific settings. Some may require fewer services to run securely, others may require more. It is recommended that you shutdown and / or disable as many services that you don't need. Windows installs many services that are configured to automatically start and are not necessarily required for proper operation of your server. Disabling as many as you can will go a long way to keep your servers secure. Also, running some services in ""manual" will still allow the service to start if needed by the Operating system. Setting some services to start manually is a good way to check and see if the Operating System is using the service. If the services are not running after several days of operation then that service may be a candidate for being disabled. The NSA template comes with no services that are configured because it is difficult to say what services can be shutdown and not cause any problems for any particular environment. Below, the services that I will configure in the NSA template as disabled are listed. As always, it is recommended that you thoroughly test these settings to make sure that no applications or server operations break as a result of these settings.

1. **Alerter:** used in conjunction with the messenger service it is used to display pop up administrative alerts. Since we will be monitoring the event logs for administrative alerts this service will not be needed.
2. **Automatic Updates:** this service replaced the critical update service and is installed by default with Windows 2000 Service pack 3. We will disable this service because we will be managing updates to the operating system only after testing updates in a lab. Misconfigurations of this service could allow unauthorized updates to be downloaded to the server. Thus having a service that automatically downloads software is not required or desired.
3. **Computer Browser:** Mainly used for backwards compatibility for previous versions of Windows. Since we are using Active Directory and Windows 2000 exclusively we will disable the computer browser service. If you are still using WINS then this service is still needed. Read: http://support.microsoft.com/?kbid=188001 for more info.

4. **Clip book:** The clip book service allows remote viewing of the clipbook pages by remote computers. This service is disabled because this functionality is not required.
5. **Fax service**: this server is not a fax server and will never receive or send faxes. Service was disabled.
6. **Indexing service:** this service creates indexes of files so that the files can be easily searched. This service has been exploited numerous times on web servers and is not needed on this file server as the potential risks outweigh the need to keep it running.
7. **License Logging service:** This service only needs to run on a domain controller.
8. **Messenger:** sends and receives messages by the alerter service. This service also displays the current user that is logged on to the computer using the NBTSTAT utility. This service will be disabled to prevent remote users from using NBTSTAT to "see" who is logged on the server.
9. **NT LM Security Support provider:** Provides NTLM security for RPC for NTLM authentication. We will only have windows 2000 and above clients plus we don't allow NTLM under the security options setting, so this service is not needed.
10. **Remote Access Auto connection manager:** This service is only required for servers that have a dial-up connection as it will offer to dial a connection when remote networks are unavailable. We will disable this service as it is not needed.
11. **Routing and remote access:** allows the server to forward packets to remote networks and is usually installed on VPN servers for remote access. This service will be disabled on this server.
12. **Telephony:** The telephony service is required for IP voice and telephony API (TAPI), there is no IP voice or modems connected toe the server so this service is disabled.
13. **Telnet:** This service allows remote access to the command shell for remote servers, but sends data in clear text. As a result, this service will be disabled. Use an SSH2 client / server product if you need Telnet function on Windows 2000.

With these services set to be disabled by the GPO for our OU we also need to make sure that regular "users" cannot change the "State" of all services. When you set a service to be disabled make sure that you also change the "access" or "permissions" of who can start and stop or otherwise manage the service. This goes for <u>all services</u> not just the disabled ones. Fro example, Branch managers will be allowed to stop and start the print spooler if needed for local printing. This will be accomplished by adding the branch managers with permission to stop start, and pause the spooler service. The steps below show how to change the permissions for any service.

Remove everyone from the "Security" settings for the service.

Go to the system services section in the Template settings section, Right click on the service that you want to configure, Chose the "define this setting… checkbox, click on edit security and remove the "Everyone" group and replace with more appropriate group(s). Check the start, stop and pause checkbox to allow the

authorized users to manage the service then move on to the next service. See figure 13 below for a screenshot.

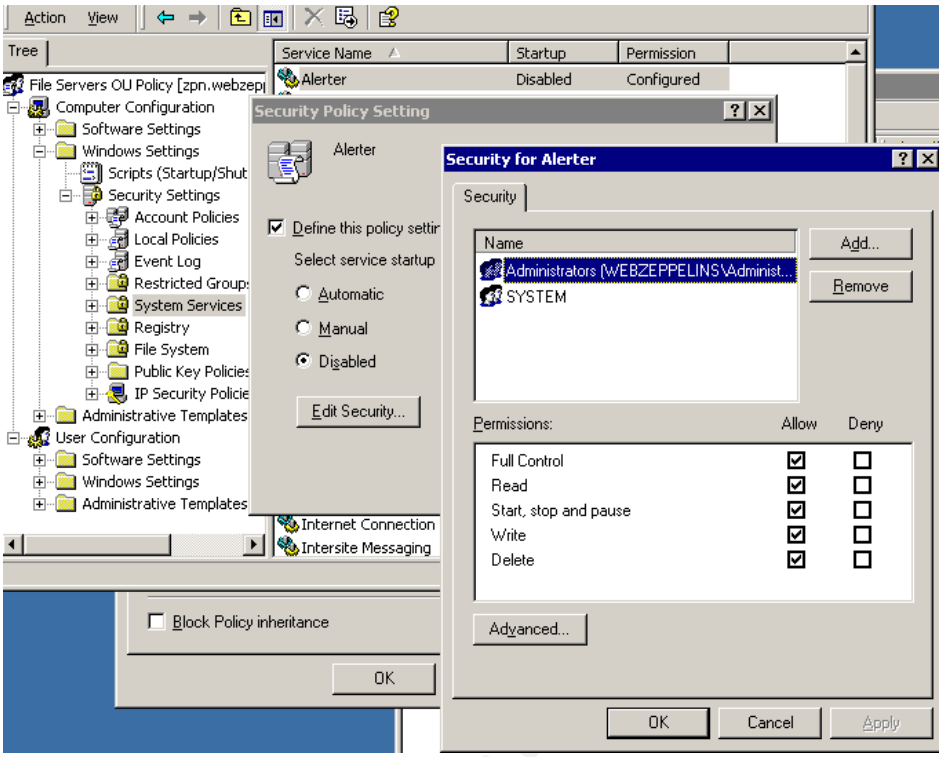


Figure 13

Registry Settings

The registry settings that are configured by the NSA template are sufficient for this file server and its environment. I will be removing the “backup operators” from the “HKLM/System/CurrentControlSet/Control/SecurePipeServers/Winreg” key in the registry section of the security template. Remote access to the registry is controlled by this key and allows remote access for groups or users that have permission here. The administrators group will be the only group with permission to this key. The permissions that are set by the template are located in Appendix B.

File System Permissions

The file system permissions that are configured with the NSA template will definitely need to be further enhanced. We will remove the “users” group from the template and replace it with the “branch managers” group. This change will allow members of the “branch managers” group READ access to most server settings without having to place the branch managers into the local administrators group while they are logged on locally to the server. This is a way to allow trusted users local access to files without risking server operations by using a “generic” group like “users” in the file system ACL’s. The “users group also contains the “authenticated users” group and we would like more control of the server. Because only privileged users are members of the Branch managers group, making this change will greatly enhance the servers’ security. The file permissions that are configured for this server are shown in Appendix C.

Enhanced file security

Although the settings in appendix C are secure, I have opted to further enhance the file server's security by changing the ACL on the following critical system executables. All of these files will be configured with

Administrators: Full Control
System: Full Control

And will not inherit from the parent. Of course any file could be added to this list not just the files shown here.

cmd.exe	net1.exe	telnet.exe
arp.exe	netsh.exe	tftp.exe
at.exe	netstat.exe	tracert.exe
atsvc.exe	nslookup.exe	tskill.exe
attrb.exe	ping.exe	uninst.exe
cacls.exe	poledit.exe	wscript.exe
clpsrv.exe	posix.exe	xcopy.exe
command.exe	qbasic.exe	
cscript.exe	qfecheck.exe	
debug.exe	rcp.exe	
dialer.exe.exe	rdisk.exe	
edit.exe	regedit.exe	
edlin.exe	regedt32.exe	
finger.exe	regini.exe	
ftp.exe	regsvr32.exe	
hypertrm.exe	rexec.exe	
htimage.exe	route.exe	
imagemap.exe	rsh.exe	
ipconfig.exe	runas.exe	
issync.exe	runonce.exe	
msiexec.exe	secfixup.exe	
nbtstat.exe	sysedit.exe	
net.exe	syskey.exe	

Figure 15

Note: You can also move executables to a separate directory and ACL the directory to the desired level and this represents a known good practice, but if you choose to do this you must also make sure that those files are also removed from the hidden folder %SYSTEMROOT%DLLCACHE or the windows file protection service will simply replace the files that were moved. Then what can happen is you will have the files that you moved to your "secured" directory, and also those same files will be automatically replaced in the system folders that you removed them from, and they will inherit permission from the parent, which may include users that you do not want to have access to those files. This is why I recommend that you specifically assign permissions to the files directly in the %SYSTEMROOT%\System32 directory. This way the proper permissions will still be assigned to the files and you don't have to worry about removing them from the DLLCACHE folder. If the files are accidentally deleted for one reason or

another those files will still get the proper permission on the next refresh of the GPO. This is a simple way to ensure that the critical exe files that you want to restrict will always have the correct permissions. I added these files to the template and changed the permissions to Administrators: FULL and System: FULL With Replace. **For more information on the windows file protection service please refer to: KB article** http://support.microsoft.com/?kbid=229656

To add these extra files to your template, navigate to the file system area of the template then right click the File System folder, choose add file… navigate to the file that you want to secure and choose the proper permissions. Then make sure to choose the replace and propagate radio button. Don't check the "allow inheritable permissions to propagate form parent" checkbox.

One other word of caution, When you apply a service pack to Windows, using the network install file that is downloaded from Microsoft, and execute it directly on the machine to be updated, you may see a new folder created in %systemroot% called \servicepackfiles\i386 this directory can also contain files that need to be secured (i.e.ftp.exe, etc…) This directory is created so that you don't need to reinstall the service pack when new services like DNS, WINS or DHCP are added after the service pack was installed. In order to make sure that the critical files we are protecting with enhanced ACL cannot be executed from this directory we will need to also ACL this directory with the same permissions as the critical files above. Please refer to http://support.microsoft.com/default.aspx?scid=KB;en-us;q290728 for more information on this issue as there are a couple of workarounds to this. Protecting files in the system32 directory can be tricky because of the system file protection service.

Once you have all the files you want to add to the template you are finished with the configuration and now we need to save this template as a new file.

Simply right click the Template we have just finished configuring and choose Save as…

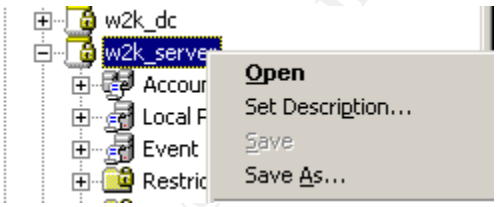


Figure 17

Choose a name for the template…

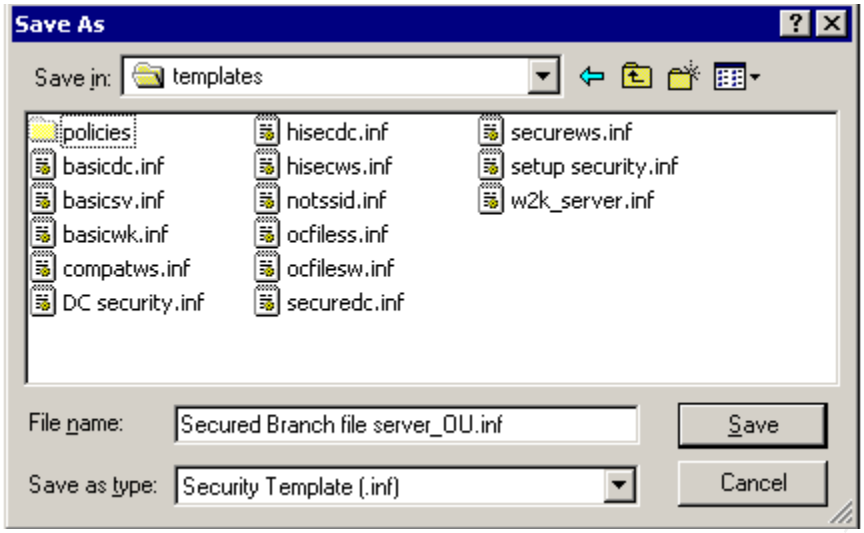


Figure 18

Here we have chosen to name the GPO template with _OU on the end of the name. This way it will be easy to see which OU's the GPO's should be applied.

Apply the Template

Now we will apply this template to our File server OU within the Active Directory

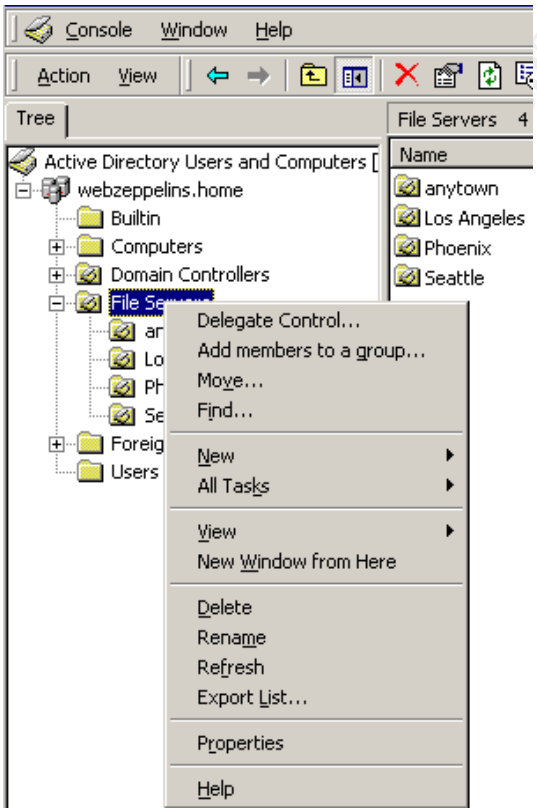


Figure 19

Open the Users and Computers MMC and navigate to our File server OU. Then right Click the OU that we want to secure. In our case it is the File servers OU. Go to properties from the drop down list and choose the Group Policy tab. From this choose new, once this is done you will have a new blank group policy created. Rename this policy to a descriptive name. We have re-named ours to Secured Branch File servers_ OU policy. Then click on the edit button, this will open a window so that we can import the new template that we created earlier. See figure 20.

You can also apply the template that we created directly to a server by opening the “local security policy” tool under the administrative tools section of the program menu. Since our server belongs to an Active Directory, Security templates are better managed through Group Policy.

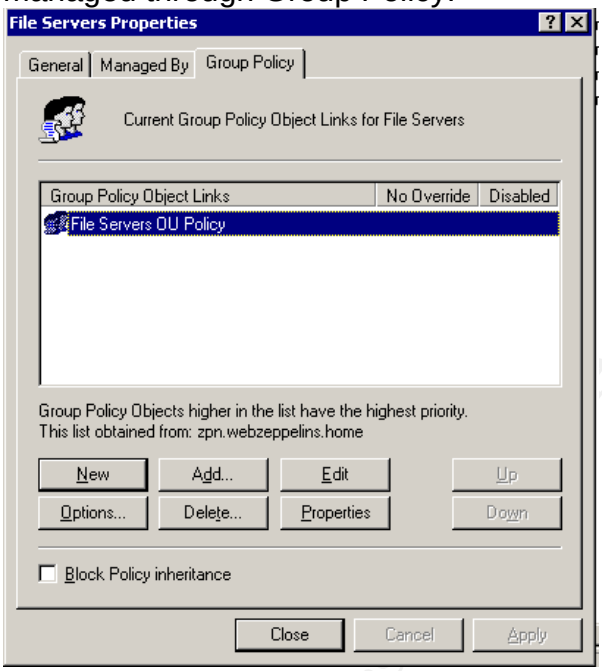


Figure 20

Once the edit button has been clicked you are presented with a way to import your new GPO template.

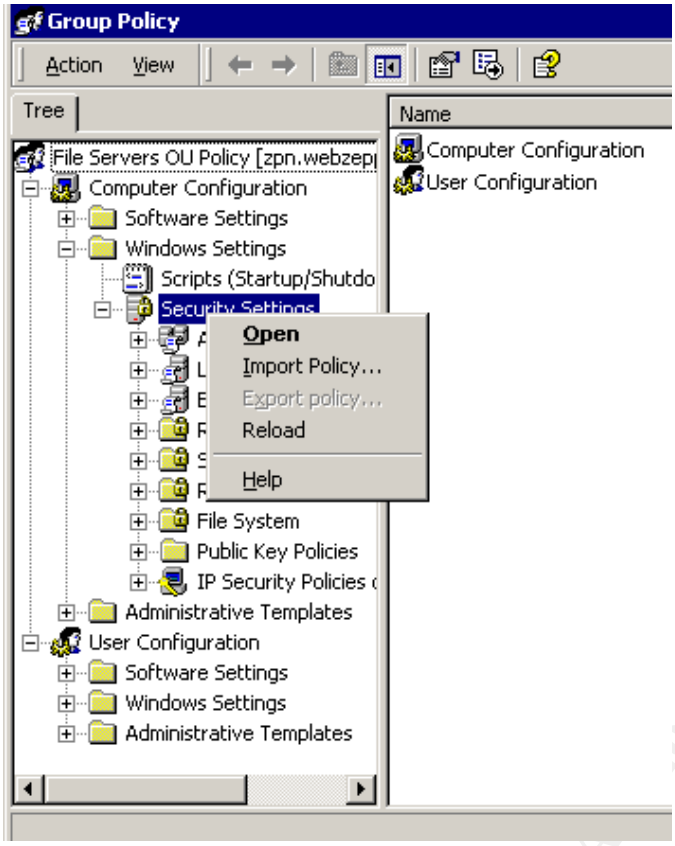


Figure 21

Expand computer Configuration > Security Settings then right click and choose Import Policy.

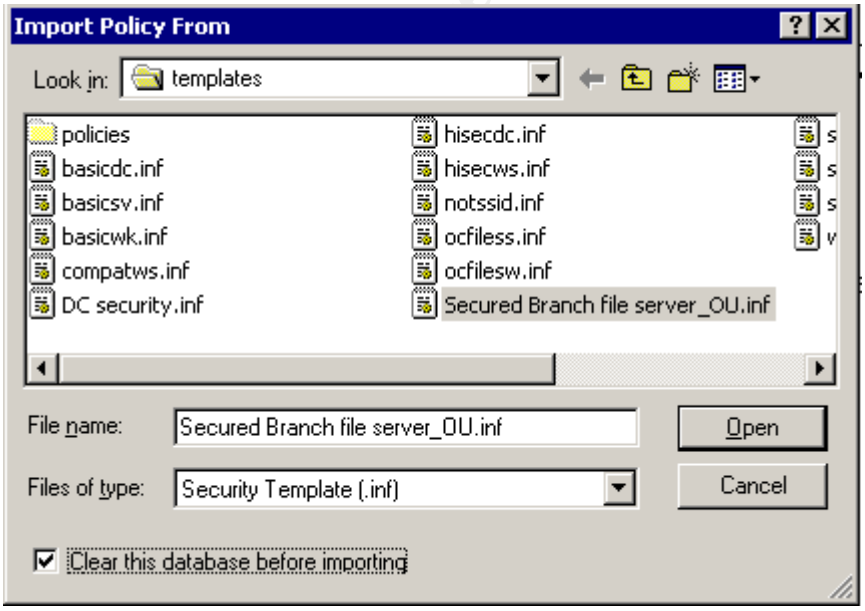


Figure 22

Choose the secured Branch file server_OU.inf file, check the clear this database before importing box and click open. This will import the GPO to the OU. Now all servers located in the File servers OU will receive this policy by inheritance. Once the GPO has been imported, by default it is refreshed every 90 minutes or every time a server is rebooted. You can change the refresh interval in the template under the Administrative Templates>System>Group Policy, in the GPO, under this folder section there is a policy to activate called ***"Group Policy refresh interval for computers"*** Here you can set the group policy to automatically refresh from 0 -64800 minutes (45 days). This setting is very handy when you want to refresh the policy more or less often than the default 90 minutes. I will configure this setting to 1 hour +-15 minutes for randomness. In the event that a setting configured by the File servers GPO was changed, approximately 60 minutes later the setting would be reset to the original value.

Test the template's security settings

To make sure that the GPO security is applied, we will look at several items.

1. A logon banner warning users that this system is for "authorized use only" sends a clear message to users and can aid you in court if you need to take legal action. Before the GPO was applied there was no warning or Logon Banner for this server. After applying the template we now we see a logon banner on the server prior to logging in. This is effective because it allows you to have a consistent logon banner across the enterprise and can be customized for specific servers that need it. Since it is applied at the OU level you can use different logon banners for workstations and servers if needed, or simply this could be applied at the domain level as well for consistency.

Below is just a sample of text you can put into the logon banner, you may want to talk to your legal department for guidance on the wording.

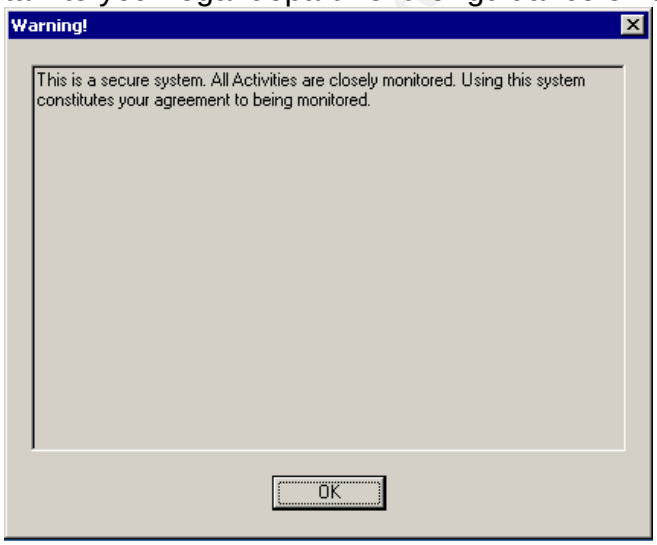


Figure 23

2. Critical File Security.

   In our template we added a list of critical files (see figure 15) that needed to be executed only by System administrators. Since branch managers were going to be able to logon locally to the server we needed to make sure that these "critical" files could not be executed by members of the Branch Managers group. Branch managers are not part of the local administrators group and only perform basic server maintenance such as manually backing up files or stopping and starting the print spooler service locally. We will check these critical files to make sure that security was applied as expected. See Figure 24.

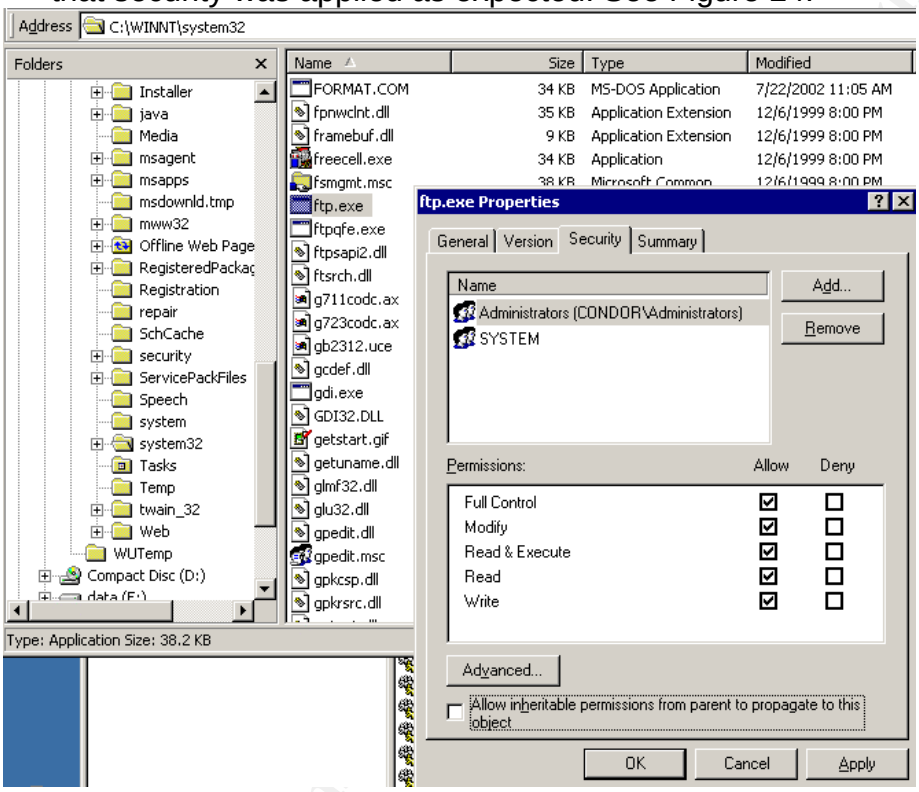


Figure 24

As you can see from the screenshot above, the ftp.exe file permissions were changed to Administrators and SYSTEM only and do not inherit permissions from the parent folder. All of the files on the critical file list received this setting. This setting is important because the branch managers are not a member of the local administrators group and we do not want Branch managers executing these critical files. To further test this we logged on to the server as the user branchmanager1. We then tried to copy the FTP.exe file to the desktop and temp folders. The result was that we were denied access to copy the file or execute it.

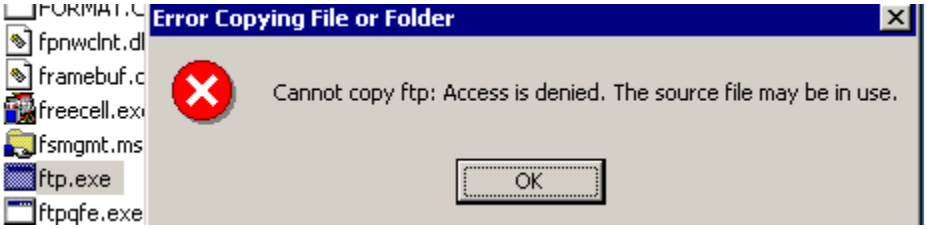
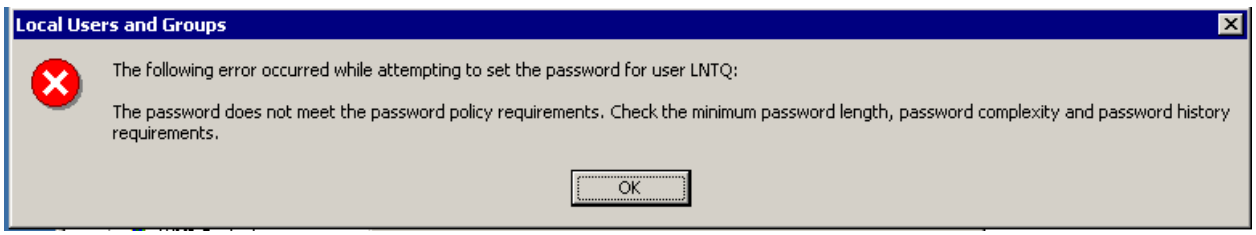


Figure 25

Password Policy

Our Domain password policy is set to remember 8 passwords, have a minimum of 8 characters, must be complex and must be changed every 90 days. I think that reducing the character count from 12 to 8 is more appropriate for our environment. 12 character passwords can be too complex for most users to remember and this fosters the habit of users to write their passwords on paper to remember them, reducing the effectiveness of a good password policy. I feel that reducing the number of characters from 12 to 8 is easier to remember. The NSA policy of 90 days maximum age is a good setting as this also will make remembering passwords without writing them down easier for the user community. With a history of 8 and passwords must be changed every 90 days will not allow a user to "re-use" any password for 2 years. If users are forced to change their passwords often then it makes remembering them much harder and creating new passwords constantly can lead to users back to the habit of writing them down on paper or creating less effective ones. I feel that creating fewer but more "thought out" passwords is better than creating lots of passwords but have less thought put into them. A good password policy is a balance of complexity and cycle, too much of one or the other can lead to users getting discouraged and making the policy less effective. The account lockout policy is 0 or forever. This is changed from the NSA recommended setting of 15 minutes. I feel that it is best for a user to have to call the help desk to get their account unlocked instead of timing out in 15 minutes and resetting automatically. This will prevent hackers using password guessing software and waiting for the account to "reset". Forcing someone to call the help desk gives more accountability and is easier to audit how often people are locking out their accounts. To test whether the Domain password policy was applied properly to the server we will try to change the password of the local administrator account to something less than desired or permitted. When I tried to change my password to a 7 character password that included Upper and lower case letters and 1 number I got an error shown in the screenshot, the password was QwErty5



When I modified the password to be longer than 8 characters the password change was successful. The successful password used was QwErty12#

Remember that I did not create a password policy to be set by the GPO because the password policy would be inherited by the domain policy and then applied to the server. To make sure that our GPO did in fact inherit the Domain policy a screenshot is shown indicating that the settings were inherited from the Domain. Notice that the local settings shown here are what are set by default in Windows 2000 as local, but the domain policy prevails as shown here under "Effective Setting". So even though a password policy was not set in the GPO at the OU level, the Domain policy still has effect and has been applied as expected.

a. Note: Again, I chose not to configure a local password policy on this server to better illustrate that the Domain password policy was applied. Best practice would be to configure a password policy that matches your Domain Policy at the local level. The screenshot below is simply used to confirm that the policy was set as expected.

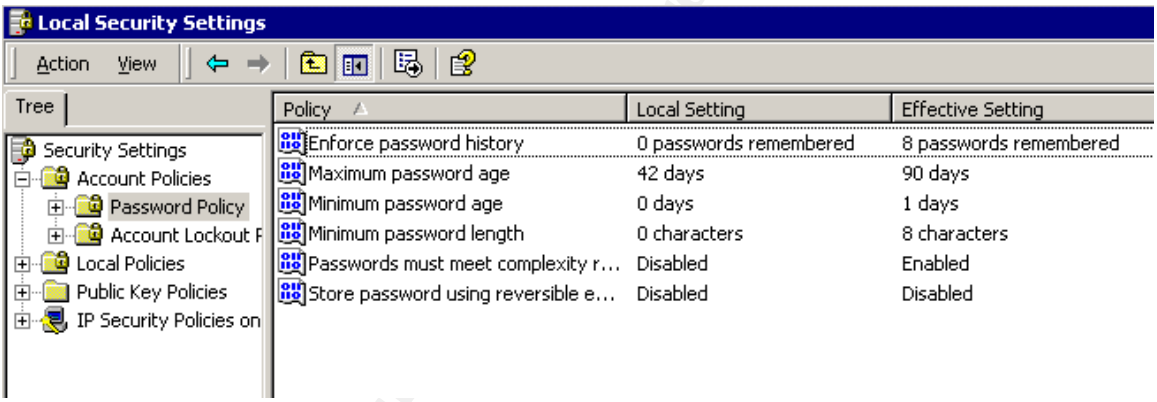


Figure 26

3. **Disabled Services**

I chose to disable several services that I knew we would not need on any file servers in the enterprise, so I disabled these services at the GPO to ensure that no file server would inadvertently start these services. All services that I disabled in the GPO policy were in fact disabled by the GPO.

The disabled services were:

Alerter	Clip Book	License Logging Service	Remote Access Auto Connection manager	Telnet
Automatic Updates	Fax Service	Messenger	Routing and remote access	

Computer Browser	Indexing Service	NT LM Security Support Provider	Telephony	

Figure 27

To test whether the services also received the correct permissions I logged on to the file server as the branch manager and tried to start a disabled service.

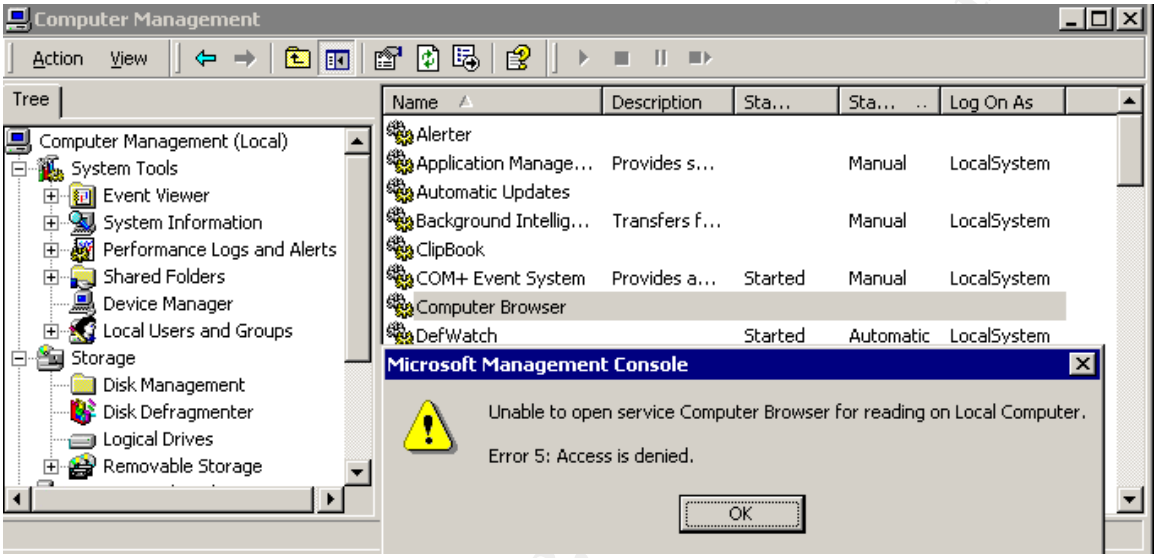


Figure 28

Access to the disabled service was denied.

Test the system functionality

To test the systems usability after applying the template I will run several tasks that are performed by users and administrators on the server to see if the servers function has been impeded by the new security settings.

Bank tellers and other branch employees need to be able to access the server to print documents for customers to sign, save their work to their home drives and get to the common drive for shared group files etc… When users logon they run logon scripts that map the common file areas.

I logged on as Teller1 to test this and see if the business users still had the same functionality to do their jobs.

1. Logged on as Teller1 I was able to get into my “home Drive” with full control. Access to the user’s home drives are managed in the profile section of the user account.

2. Logged on as Teller1 to test printing and I was not able to print to the office printer anymore. Print jobs would fail. The problem came from replacing the "users" group in the file system configuration with the Branch managers group for tighter security. Because regular "users" are not permitted to logon locally the "users" group was not needed in the file system and was replaced with the Branch manager group to enhance the security of the system. This problem was resolved by creating a local group called "any town branch users" and populating it with the branch employees, and then I had to add permission for read access to the *C:\WINNT\system32\spool* directory. After adding this new local group with the branch users that needed to print I was then able to print successfully to the office printers again. This change will be made to the template as well.
3. Logged on as Teller1: There is a common shared file area on the server that has the branch policies and procedures, business documentation, business forms, signature cards for signature verification and a digital drop box that all users have write access but not read access and is used as a virtual suggestion box at the branch.. This shared common file area was not configured by the security template as its needs are fairly dynamic and are managed manually by the home office administrators. It is located on a separate partition and was still accessible to all users with permission.
4. Logged on as administrator: I logged on as a domain administrator via terminal services (only used for remote administration) and tested the system for usability. All actions that were performed by the administrator succeeded. Actions performed were stopping and starting services, rebooting the server clearing the security event logs all were successful.

5. As administrator I was able to change the state of a service that was disabled by the GPO showing that administrators are not prevented from making system changes that are disabled for other users (i.e. Branch Managers) and still retain full control over the server. See figure 29.

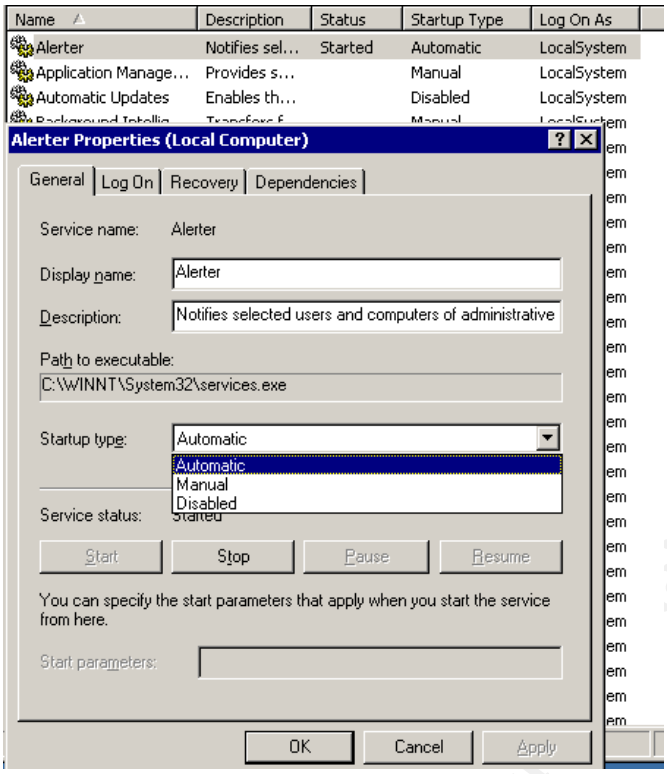


Figure 29

6. Logged on as administrator I was able to see the contents of the security logs, this is not available to non administrators.

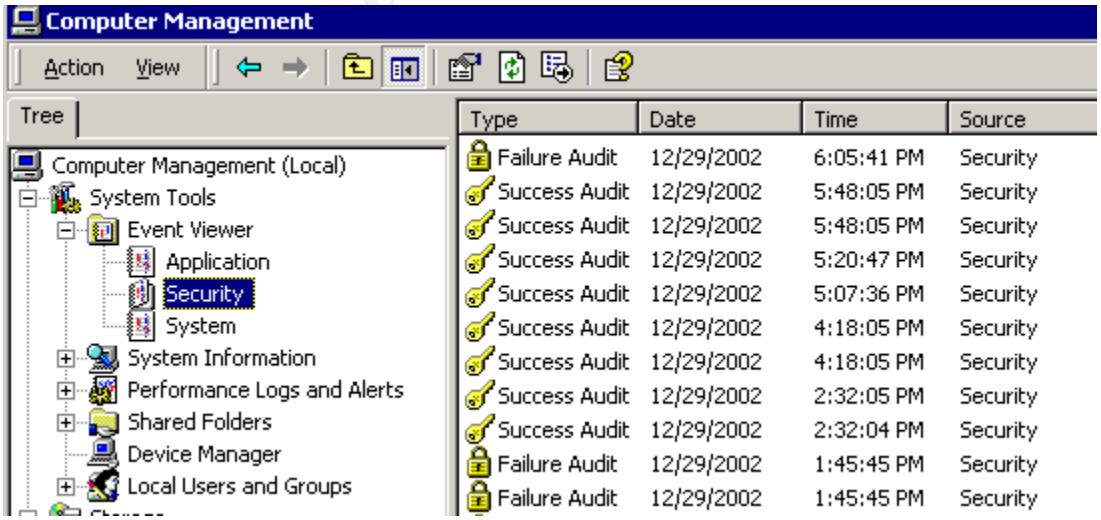


Figure 30

7. Logged on as an administrator I was able to open a restricted executable file: regedt32.exe this is one of the “restricted” files that was added to and then

configured by the template.

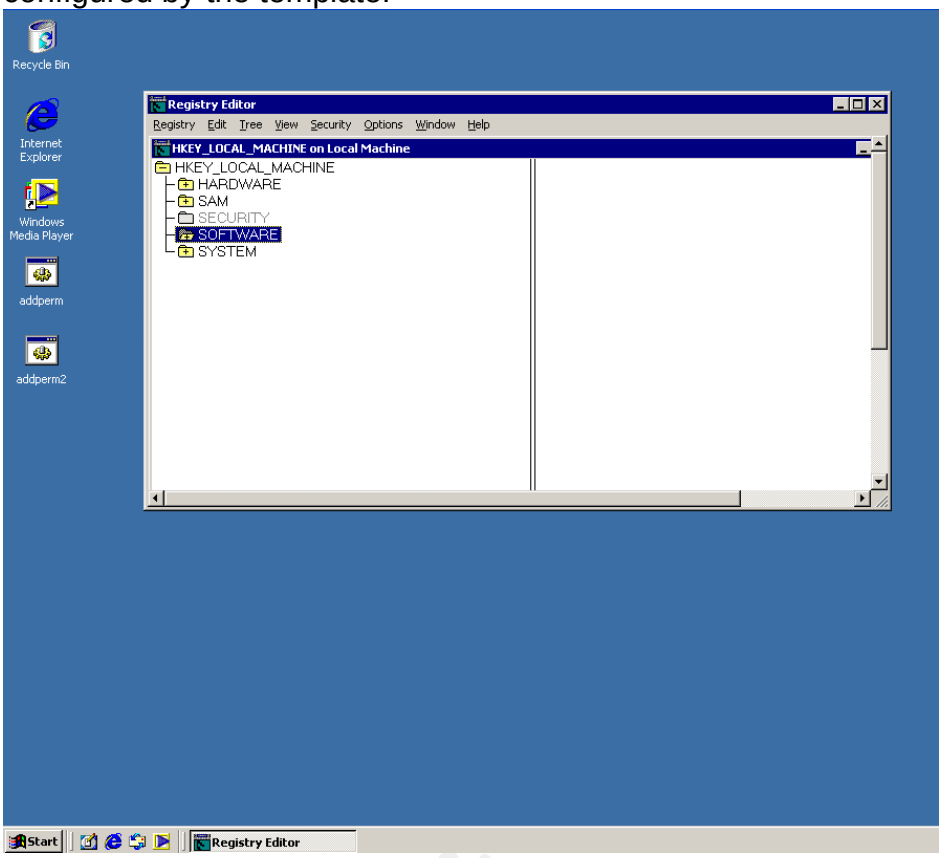


Figure 31

. **Verify restricted access**
Branch Managers will not have much of a reason to logon to the servers but may be called upon to logon locally by remote administrators, or maybe need to restart the spooler service to free a stuck print queue. Since these users are allowed to logon locally we must be sure that branch managers can not make changes to the server unless directed by systems administrators at the Home Office. If necessary, Branch Managers could use the “runas” feature to execute restricted programs using a temporary administrative account created for this purpose. This account will be disabled unless needed.

I will logon to the file server locally as a member of the branch managers group and test the restrictions for this group.

Part of the “Branch manager’s job will be to ensure that users can print to the local printers at the branch. If the print spooler queue hangs the branch manager will need to be able to restart the spooler service. When I configured the services section of the template I added the branch managers group with permission to stop and start the spooler service, I will now test whether the branch manager can perform this task.

Once logged on to the server locally as the branch manager I was able to successfully stop and start the spooler service yet I was not able to start or stop any other service, this is by design and is behaving as expected.

1. As the branch manager I will try to access the security logs:
   I was unable to view any security logs.

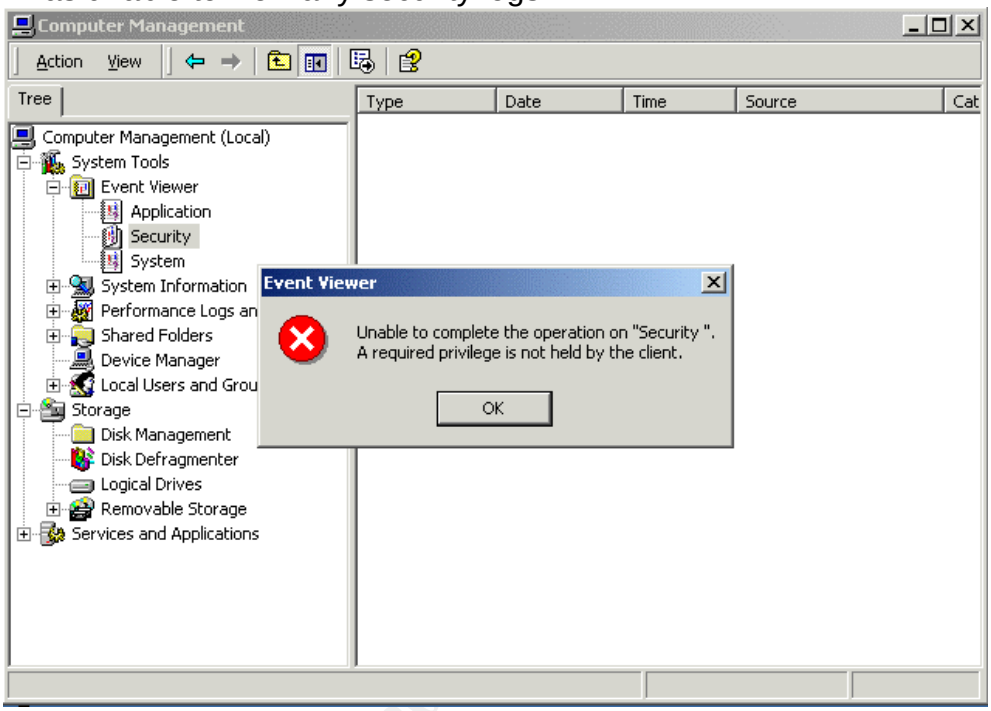


Figure 32

2. The branch manager user is also unable to connect remotely through terminal services. For all branch manager access, local logon is required and terminal access is prohibited.

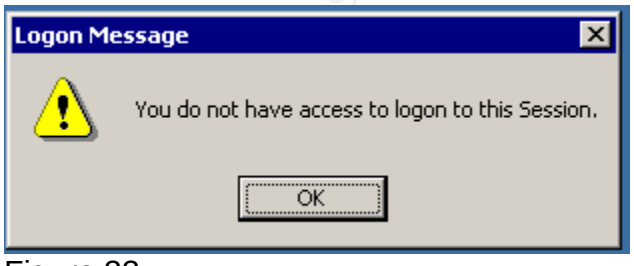


Figure 33

3. When the branch manager user tries to execute the backup program access is denied.

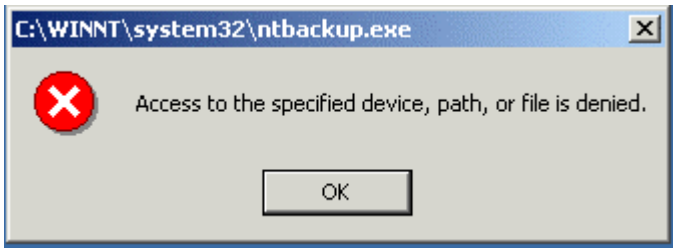


Figure 34

4. Now the branch manager will try to access the backup program using runas. By navigating to the backup program in the program menu, holding down the shift key then right clicking a new option “runas” will appear. By choosing runas we can give the branch manager temporary access to a protected program without adding him to the local administrators group.

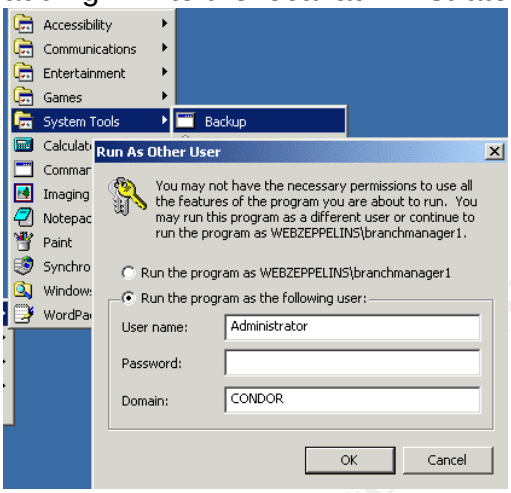


Figure 35

This time the branch manager was able to access the backup program. By using the runas option, you can give remote administrators the ability to allow local trusted users (branch managers) elevated access to certain parts of the system without having to put the user in the local administrators group. The Runas option allows only that single action to be performed. As soon as the branch manager is finished with the task, the runas user that he logged on with can be disabled or the password changed to prevent him from using it again unless he calls someone that can enable the user again.

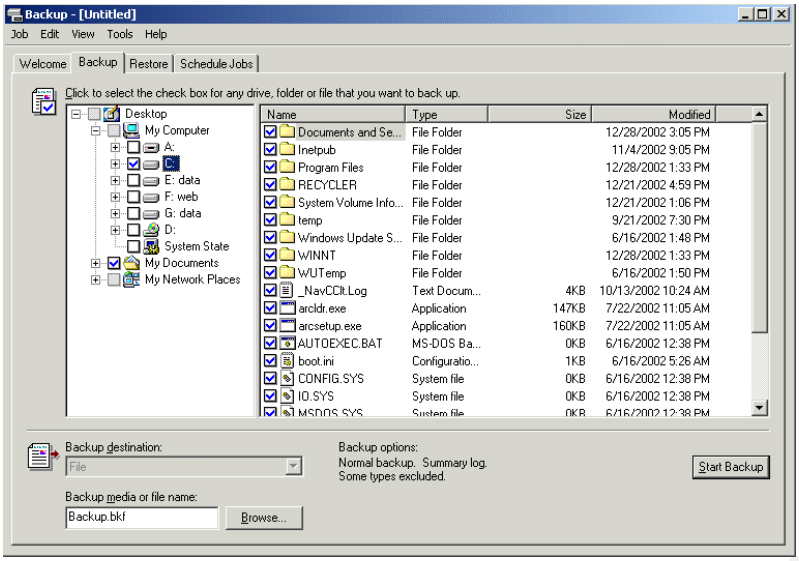


Figure 36

5. The branch manager has access to the anti virus program and is able to scan files locally if needed, but is unable to change the settings set by the administrator as shown in the screenshot below. (Figure 37)

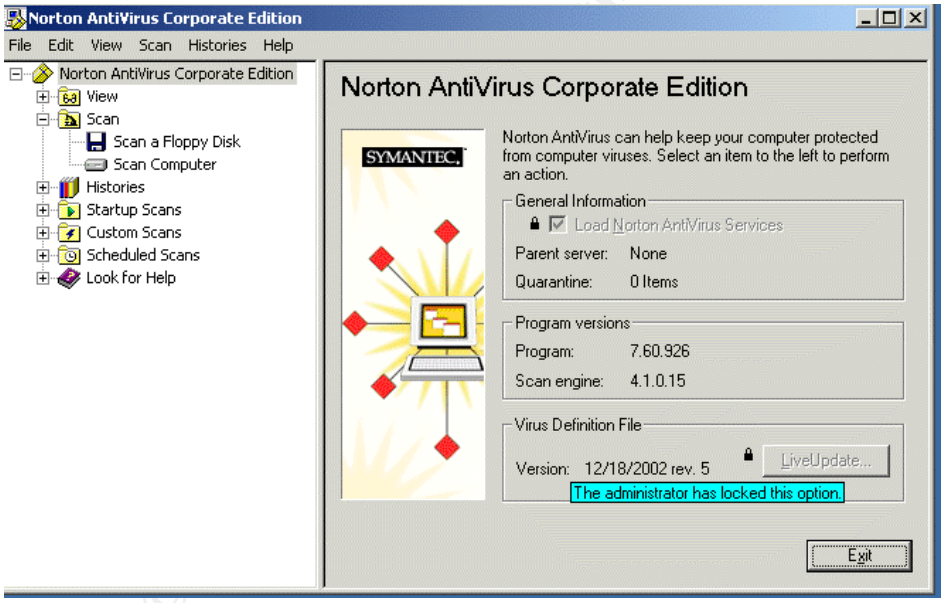


Figure 37

6. Finally, the branch manager is not allowed to shutdown the system only logoff.

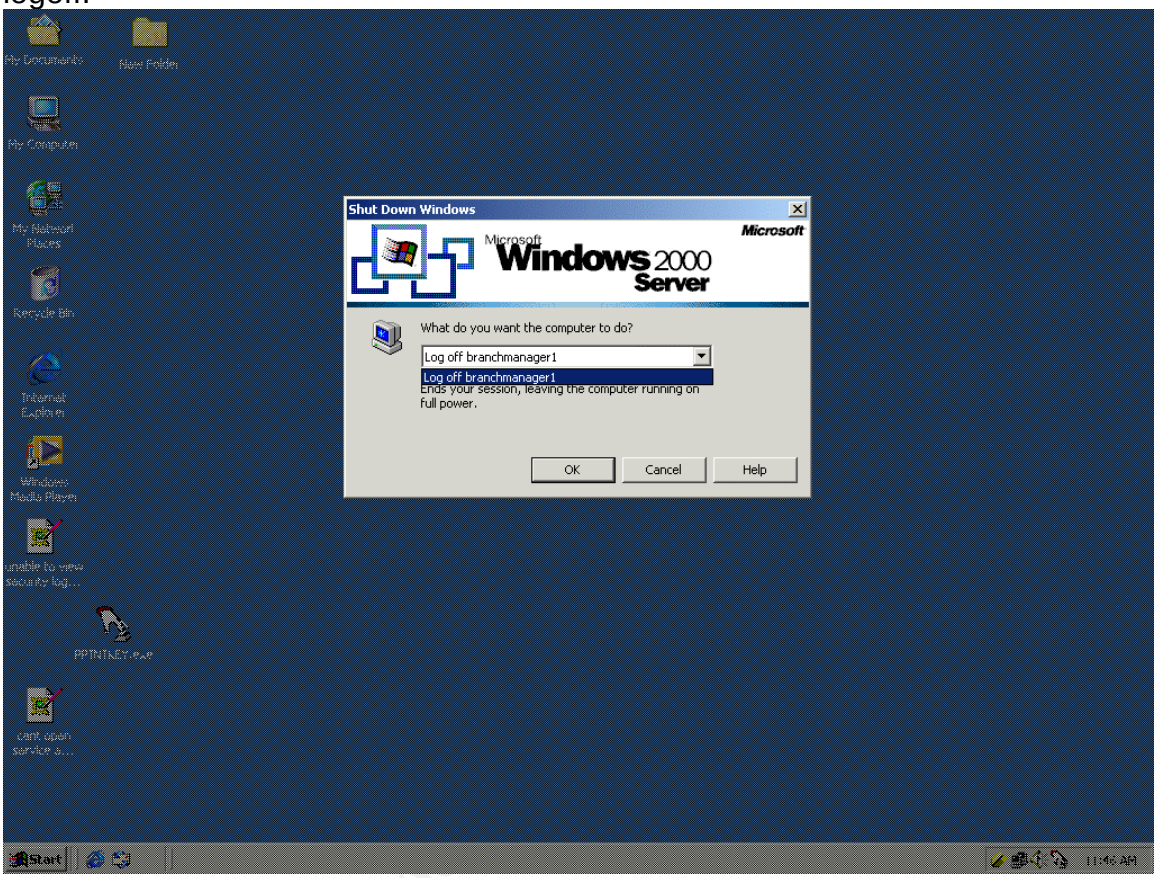


Figure 38

As you can see by the tests performed here, the server is very secure and only authorized administrators are able to logon locally, make system changes, such as reboot the server, change the state of services running and accessing critical system executables. The only other authorized personnel to logon locally are the branch managers and they are very limited as to what tasks they can perform without first contacting home office for approval. Branch managers are also prevented from accessing the server via terminal services and must logon at the console. All branch users were able to still get access to their files and printers. But the print function needed to be “fixed” by placing a new local group that had the authorized personnel on the c:\winnt\system32\spool directory.

.

Evaluate the template ------- w2k_server.inf

The NSA security template I used (w2k_server.inf) is a great "baseline" template to use as a starting point to build a more secure file server. Applied as is, any Windows member file server will become very secure and only users in the local administrators group will have access to all critical functions. The password policy I believe is too strict for general purpose implementation although I do believe in a good password policy; you must strike a balance with the tolerance of your user's frustration for changing passwords too frequently and requiring long 12 characters or more in length. That is why I would recommend lowering the minimum characters for the password policy to 8 from 12. Administrators are more tolerant and understanding of strict policies for passwords and they should already be using long complex passwords when logging on to servers. The settings for the file system are good, only allowing "users" read access and this is good for ease of use, but the template could be more secure by removing the "users" group from the file permissions area all together and substitute a custom group to take the "users" place. This might break access from general users trying to access the system. If this was the default configuration and the rule of least privilege was followed the server would be "secured" out of the box and functionality would only be gained by loosening the system permissions until the functionality was brought up to the level desired. As always, the settings included by the template may still be too lenient for some environments and too tight for others as there is no universal template that can address the security requirements for all organizations, but this w2k_server.inf template can be used straight away to secure your member servers quickly, But with some tweaking to address your organizations concerns. Thorough testing, of course is a must to make sure your applications and/or system capabilities are not limited, or functions of the server "break" after the template is applied.

Though the template is very secure from the start, it can and should be customized for your environment. Also, system security can be enhanced by adding critical system executables like telnet, ftp etc… to the file system settings in the template; certain services should be disabled by default, like messenger, clip book, fax, and alerter but it is understood that as a baseline template, not disabling any services in the template is useful for being more compatible to the community as a whole.

References:

Fossen, Jason. Active Directory, DNS and Group Policy Version 5.1.3 SANS.ORG 31/December/2001

Anonymous. Maximum Windows 2000 Security. Indianapolis: Sams Publishing, Dec.2001

Lowe-Norris, Alistair G. Windows 2000 Active Directory. Sebastopol: O'Reilly and Assoc., January 2000

Internet Security Systems Inc. Microsoft Windows 2000 Security Technical Reference Redmond: Microsoft Press, 2000

Jennings, Rodger. Admin 911 "Windows 2000 Group Policy". Berkley: Osborne. 2001

Microsoft Corporation "Securing Windows 2000 File and Print Resources" Posted: March 13, 2001 Whitepaper
http://www.microsoft.com/windows2000/techinfo/planning/incremental/securenetworkresources.asp

Microsoft Corporation "Security Settings"
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/615.asp

Microsoft Corporation "Windows 2000 Services" July 2001
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/prodspecs/win2ksvc.asp

Microsoft Knowledge Base Article - 271484 11/October/2002
http://support.microsoft.com/default.aspx?scid=KB;en-us;271484&

Microsoft Knowledge Base Article - 290728
http://support.microsoft.com/default.aspx?scid=KB;en-us;q290728

Appendix A:

NSA File server template before modifications

```
; (c) Microsoft Corporation 1997-2000
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name:        W2k Server.INF
; Template Version:     05.00.DR.0000
;
; Revision History
; 0000  -        Original
; May 2001 - SNAC version 1.01a
; November 2001 -
```

```
;       Changed the line "RequireLogonToChangePassword = 1" to
;       "RequireLogonToChangePassword = 0" under the [System Access]
;       section. This line is an artifact from Windows NT 4.0 templates and could have
;       adverse effects on a user's ability to change password at first logon. If you have
;       experienced this problem, please reapply this corrected inf file, or, via a
;       text editor, create and apply an inf file with only the following lines:
;       [Unicode]
;       Unicode=yes
;       [System Access]
;       RequireLogonToChangePassword = 0

;
;       NOTE: This setting does NOT appear when the template file is viewed
graphically in
;       the MMC.
;
; ; July 2002 -
;       In the Registry section, corrected the
;       MACHINE\System\CurrentControlSet\Control\Wmi\Security to grant
Administrators Full
;       Control on the key and subkeys
;
; Warning : Care should be exercise When using this template on Exchange Server
platform.
;        Additional settings and modification to these settings are required, which are site
specific.
;        No general .INF templates are available for Exchange Server on Windows 2000
at this time.


[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 90
MinimumPasswordLength = 12
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 15
LockoutDuration = 15
RequireLogonToChangePassword = 0
ClearTextPassword = 0
[System Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
```

```
RetentionDays = 7
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 2
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 0
AuditDSAccess = 0
AuditAccountLogon = 3
CrashOnAuditFull = 1
[Version]
signature="$CHICAGO$"
Revision=1
[Privilege Rights]
seassignprimarytokenprivilege =
seauditprivilege =
sebackupprivilege = *S-1-5-32-544
sebatchlogonright =
sechangenotifyprivilege = *S-1-5-32-545
secreatepagefileprivilege = *S-1-5-32-544
secreatepermanentprivilege =
secreatetokenprivilege =
sedebugprivilege =
sedenybatchlogonright =
sedenyinteractivelogonright =
sedenynetworklogonright =
sedenyservicelogonright =
seenabledelegationprivilege =
seincreasebaseprioritypriviledge = *S-1-5-32-544
seincreasequotaprivilege = *S-1-5-32-544
seinteractivelogonright = *S-1-5-32-544
seloaddriverprivilege = *S-1-5-32-544
selockmemoryprivilege =
```

semachineaccountprivilege =
senetworklogonright = *S-1-5-32-545,*S-1-5-32-544
seprofilesingleprocessprivilege = *S-1-5-32-544
seremoteshutdownprivilege = *S-1-5-32-544
serestoreprivilege = *S-1-5-32-544
sesecurityprivilege = *S-1-5-32-544
seservicelogonright =
seshutdownprivilege = *S-1-5-32-544
sesyncagentprivilege =
sesystemenvironmentprivilege = *S-1-5-32-544
sesystemprofileprivilege = *S-1-5-32-544
sesystemtimeprivilege = *S-1-5-32-544
setakeownershipprivilege = *S-1-5-32-544
setcbprivilege =
seundockprivilege =
[Group Membership]
*S-1-5-32-547__Memberof =
*S-1-5-32-547__Members =
[Registry Values]
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1
machine\software\microsoft\driver signing\policy=3,1
machine\software\microsoft\non-driver signing\policy=3,1
machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\securitylevel=4,0
machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\setcommand=4,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatecdroms=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\allocatedasd=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatefloppies=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\cachedlogonscount=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\passwordexpirywarning=4,14
machine\software\microsoft\windows nt\currentversion\winlogon\scremoveoption=1,1
machine\software\microsoft\windows\currentversion\policies\system\disablecad=4,0
machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername=4,1
machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon=4,0
machine\system\currentcontrolset\control\lsa\auditbaseobjects=4,1
machine\system\currentcontrolset\control\lsa\crashonauditfail=4,1
machine\system\currentcontrolset\control\lsa\fullprivilegeauditing=3,1
machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel=4,5
machine\system\currentcontrolset\control\lsa\restrictanonymous=4,2

machine\system\currentcontrolset\control\print\providers\lanman print services\servers\addprinterdrivers=4,1
machine\system\currentcontrolset\control\session manager\memory management\clearpagefileatshutdown=4,1
machine\system\currentcontrolset\control\session manager\protectionmode=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect=4,30
machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature=4,0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpassword=4,0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysignature=4,1
machine\system\currentcontrolset\services\lanmanworkstation\parameters\requiresecuritysignature=4,0
machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange=4,0
machine\system\currentcontrolset\services\netlogon\parameters\requiresignorseal=4,0
machine\system\currentcontrolset\services\netlogon\parameters\requirestrongkey=4,0
machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel=4,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=4,255
[Profile Description]
Description=NSA Enhanced Security for Windows 2000 Member/Stand-alone Servers
[File Security]
"%SystemDrive%\Program Files\Resource Kit",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\security",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\Default User",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\ntldr",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\config.sys",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\ntdetect.com",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\boot.ini",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\autoexec.bat",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\$NtServicePackUninstall$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"c:\boot.ini",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"

"c:\ntdetect.com",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntldr",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntbootdd.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\autoexec.bat",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"c:\config.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%ProgramFiles%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OI
CI;0x1200a9;;;BU)"
"%SystemRoot%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OIC
I;0x1200a9;;;BU)"
"%SystemRoot%\CSC",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\debug",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)
(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\Registration",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;FR;;;
BU)"
"%SystemRoot%\repair",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\Tasks",1,"D:AR"
"%SystemRoot%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)
(A;CI;0x100026;;;BU)"
"%SystemDirectory%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A
;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\appmgmt",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1
200a9;;;BU)"
"%SystemDirectory%\DTCLog",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;F
A;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\GroupPolicy",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(
A;OICI;FA;;;SY)"
"%SystemDirectory%\NTMSData",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\Setup",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200
a9;;;BU)"
"%SystemDirectory%\ReinstallBackups",1,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU
)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\repl",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a
9;;;BU)"
"%SystemDirectory%\repl\import",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1301bf;;;RE)(A;
OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\repl\export",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;RE)(A;
OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\spool\printers",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OI
CI;FA;;;SY)(A;CI;DCLCSWWPLO;;;BU)"
"%SystemDirectory%\config",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\dllcache",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;C
O)"
"%SystemDirectory%\ias",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDrive%\Documents and
Settings",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"

"%SystemDrive%\My Download
Files",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1201bf;;;
BU)"
"%SystemDrive%\System Volume Information",1,"D:PAR"
"%SystemDrive%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)
(A;CI;DCLCWP;;;BU)"
"%SystemDrive%\",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OI
CI;0x1200a9;;;BU)"
"%SystemDrive%\IO.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a
9;;;BU)"
"%SystemDrive%\MSDOS.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1
200a9;;;BU)"
"%SystemRoot%\regedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\rcp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\Ntbackup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\rexec.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\rsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\regedt32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\debug\UserMode",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;;CCD
CWP;;;BU)(A;OIIO;DCLC;;;BU)"
"%SystemDrive%\Documents and
Settings\Administrator",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;
;SY)(A;OICIIO;DCLCWP;;;BU)(A;OICI;CCSWWPLORC;;;BU)"
"%SystemDirectory%\secedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\Inetpub",1,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;S
Y)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson\drwtsn32.log",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;C
O)(A;OICI;FA;;;SY)(A;OICI;0x1301bf;;;BU)"
"%SystemRoot%\Offline Web Pages",1,"D:AR(A;OICI;FA;;;WD)"
"%SystemDrive%\Documents and Settings\All
Users",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
[Registry Keys]
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AsrCommands",2,"D:PAR(A;CI;KA;;;BA)(A;CI;CCDCLCSWRPSDR
C;;;BO)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for
NT",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"machine\software",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;B
U)"
"machine\software\microsoft\netdde",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
"machine\software\microsoft\protected storage system provider",1,"D:AR"

"machine\software\microsoft\windows
nt\currentversion\perflib",2,"D:P(A;CI;GR;;;IU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;C
O)"
"machine\software\microsoft\windows\currentversion\group
policy",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
"machine\software\microsoft\windows\currentversion\installer",0,"D:PAR(A;CI;KA;;;BA)(
A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\software\microsoft\windows\currentversion\policies",0,"D:PAR(A;CI;KA;;;BA)(
A;CI;KR;;;AU)(A;CI;KA;;;SY)"
"machine\system",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;B
U)"
"machine\system\clone",1,"D:AR"
"machine\system\controlset001",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY
)(A;CI;KR;;;BU)"
"machine\system\controlset002",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY
)(A;CI;KR;;;BU)"
"machine\system\controlset003",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY
)(A;CI;KR;;;BU)"
"machine\system\controlset004",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY
)(A;CI;KR;;;BU)"
"machine\system\controlset005",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY
)(A;CI;KR;;;BU)"
"machine\system\controlset006",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY
)(A;CI;KR;;;BU)"
"machine\system\controlset007",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY
)(A;CI;KR;;;BU)"
"machine\system\controlset008",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY
)(A;CI;KR;;;BU)"
"machine\system\controlset009",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY
)(A;CI;KR;;;BU)"
"machine\system\controlset010",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY
)(A;CI;KR;;;BU)"
"machine\system\currentcontrolset\control\securepipeservers\winreg",2,"D:PAR(A;CI;K
A;;;BA)(A;;KR;;;BO)(A;CI;KA;;;SY)"
"machine\system\currentcontrolset\control\wmi\security",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO
;KA;;;CO)(A;CI;KA;;;SY)"
"machine\system\currentcontrolset\enum",1,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;
KA;;;SY)"
"machine\system\currentcontrolset\hardware
profiles",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"users\.default",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"users\.default\software\microsoft\netdde",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
"users\.default\software\microsoft\protected storage system provider",1,"D:AR"
"CLASSES_ROOT",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;
BU)"

"MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"

NSA template after customizing the settings for our environment.

```
[Unicode]
Unicode=yes
[System Access]
RequireLogonToChangePassword = 0
NewAdministratorName = "LNTQ"
NewGuestName = "zbod"
[System Log]
MaximumLogSize = 100224
AuditLogRetentionPeriod = 1
RetentionDays = 7
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 100224
AuditLogRetentionPeriod = 1
RetentionDays = 7
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 100224
AuditLogRetentionPeriod = 1
RetentionDays = 7
RestrictGuestAccess = 1
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 3
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 0
AuditDSAccess = 0
AuditAccountLogon = 3
CrashOnAuditFull = 0
[Privilege Rights]
seassignprimarytokenprivilege =
seauditprivilege =
sebackupprivilege = *S-1-5-32-544
sebatchlogonright =
```

sechangenotifyprivilege = *S-1-5-32-545
secreatepagefileprivilege = *S-1-5-32-544
secreatepermanentprivilege =
secreatetokenprivilege =
sedebugprivilege =
sedenybatchlogonright =
sedenyinteractivelogonright =
sedenynetworklogonright =
sedenyservicelogonright =
seenabledelegationprivilege =
seincreasebasepriorityprivilege = *S-1-5-32-544
seincreasequotaprivilege = *S-1-5-32-544
seinteractivelogonright = *S-1-5-32-544
seloaddriverprivilege = *S-1-5-32-544
selockmemoryprivilege =
semachineaccountprivilege =
senetworklogonright = *S-1-5-32-544,*S-1-5-32-545
seprofilesingleprocessprivilege = *S-1-5-32-544
seremoteshutdownprivilege = *S-1-5-32-544
serestoreprivilege = *S-1-5-32-544
sesecurityprivilege = *S-1-5-32-544
seservicelogonright =
seshutdownprivilege = *S-1-5-32-544
sesyncagentprivilege =
sesystemenvironmentprivilege = *S-1-5-32-544
sesystemprofileprivilege = *S-1-5-32-544
sesystemtimeprivilege = *S-1-5-32-544
setakeownershipprivilege = *S-1-5-32-544
setcbprivilege =
seundockprivilege =
[Registry Keys]
"MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities
",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManager
s",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"CLASSES_ROOT",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;
BU)"
"users\.default\software\microsoft\protected storage system provider",1,"D:AR"
"users\.default\software\microsoft\netdde",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
"users\.default",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\currentcontrolset\hardware
profiles",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\currentcontrolset\enum",1,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;
KA;;;SY)"
"machine\system\currentcontrolset\control\wmi\security",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO
;KA;;;CO)(A;CI;KA;;;SY)"

"machine\system\currentcontrolset\control\securepipeservers\winreg",2,"D:PAR(A;CI;KA;;;BA)(A;;KR;;;BO)(A;CI;KA;;;SY)"
"machine\system\controlset010",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset009",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset008",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset007",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset006",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset005",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset004",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset003",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset002",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset001",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\clone",1,"D:AR"
"machine\system",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\software\microsoft\windows\currentversion\policies",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
"machine\software\microsoft\windows\currentversion\installer",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\software\microsoft\windows\currentversion\group policy",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
"machine\software\microsoft\windows nt\currentversion\perflib",2,"D:P(A;CI;GR;;;IU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"machine\software\microsoft\protected storage system provider",1,"D:AR"
"machine\software\microsoft\netdde",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
"machine\software",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AsrCommands",2,"D:PAR(A;CI;KA;;;BA)(A;CI;CCDCLCSWRPSDRC;;;BO)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
[Version]
signature="$CHICAGO$"
Revision=1

[Group Membership]
*S-1-5-32-544__Memberof =
*S-1-5-32-544__Members = *S-1-5-21-347615555-2441251375-4083693081-512,*S-1-5-21-347615555-2441251375-4083693081-500
[File Security]
"%SystemDrive%\Program Files\Resource Kit",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\security",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\Default User",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICI;FA;;;SY)"
"%SystemDrive%\ntldr",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\config.sys",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICI;FA;;;SY)"
"%SystemDrive%\ntdetect.com",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\boot.ini",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\autoexec.bat",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICI;FA;;;SY)"
"%SystemRoot%\$NtServicePackUninstall$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"c:\boot.ini",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntdetect.com",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntldr",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntbootdd.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\autoexec.bat",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICI;FA;;;SY)"
"c:\config.sys",2,"D:PAR(A;;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;;FA;;;SY)"
"%ProgramFiles%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemRoot%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemRoot%\CSC",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\debug",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemRoot%\Registration",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;FR;;;BU)"
"%SystemRoot%\repair",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\Tasks",1,"D:AR"
"%SystemRoot%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;0x100026;;;BU)"
"%SystemDirectory%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemDirectory%\appmgmt",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICI;FA;;;SY)"

"%SystemDirectory%\DTCLog",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\GroupPolicy",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
"%SystemDirectory%\NTMSData",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\Setup",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\ReinstallBackups",1,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\repl",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\repl\import",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1301bf;;;RE)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\repl\export",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;RE)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\spool\printers",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;DCLCSWWPLO;;;BU)"
"%SystemDirectory%\config",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\dllcache",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\ias",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDrive%\Documents and Settings",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICI;FA;;;SY)"
"%SystemDrive%\My Download Files",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemDrive%\System Volume Information",1,"D:PAR"
"%SystemDrive%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;DCLCWP;;;BU)"
"%SystemDrive%\",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemDrive%\IO.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICI;FA;;;SY)"
"%SystemDrive%\MSDOS.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICI;FA;;;SY)"
"%SystemRoot%\regedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\rcp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\Ntbackup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\rexec.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\rsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\regedt32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\debug\UserMode",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\Administrator",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"

"%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemDirectory%\secedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\Inetpub",1,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson\drwtsn32.log",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemRoot%\Offline Web Pages",1,"D:AR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\All Users",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;S-1-5-21-347615555-2441251375-4083693081-1103)(A;OICI;FA;;;SY)"
"%SystemDirectory%\arp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\at.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\cacls.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\debug.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\edit.com",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\edlin.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\finger.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\ftp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\irftp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\tftp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\xcopy.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\net.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\ipconfig.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\nslookup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\telnet.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\nbtstat.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\ping.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\pathping.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\route.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\runonce.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\ipxroute.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\syskey.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\tracert.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\cmd.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\cscript.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\regsvr32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\runas.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\netsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\wscript.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\nwscript.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\appmgmts.dll",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\dcpromo.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"

[Registry Values]
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=4,255
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon=4,0
machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\requirestrongkey=4,0
machine\system\currentcontrolset\services\netlogon\parameters\requiresignorseal=4,0
machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange=4,0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\requiresecuritysignature=4,0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysignature=4,1
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpassword=4,0
machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature=4,0
machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect=4,30
machine\system\currentcontrolset\control\session manager\protectionmode=4,1
machine\system\currentcontrolset\control\session manager\memory management\clearpagefileatshutdown=4,1
machine\system\currentcontrolset\control\print\providers\lanman print services\servers\addprinterdrivers=4,1
machine\system\currentcontrolset\control\lsa\restrictanonymous=4,2
machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel=4,5
machine\system\currentcontrolset\control\lsa\fullprivilegeauditing=3,1
machine\system\currentcontrolset\control\lsa\crashonauditfail=4,1
machine\system\currentcontrolset\control\lsa\auditbaseobjects=4,1
machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon=4,0
machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername=4,1
machine\software\microsoft\windows\currentversion\policies\system\disablecad=4,0
machine\software\microsoft\windows nt\currentversion\winlogon\scremoveoption=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\passwordexpirywarning=4,14
machine\software\microsoft\windows nt\currentversion\winlogon\cachedlogonscount=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatefloppies=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\allocatedasd=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatecdroms=1,1

machine\software\microsoft\windows
nt\currentversion\setup\recoveryconsole\setcommand=4,0
machine\software\microsoft\windows
nt\currentversion\setup\recoveryconsole\securitylevel=4,0
machine\software\microsoft\non-driver signing\policy=3,1
machine\software\microsoft\driver signing\policy=3,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForce
dLogOff=4,1
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeTe
xt=1,This is a secure system. All Activities are closely monitored. Using this system
constitutes your agreement to being monitored.
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCa
ption=1,Warning!
[Service General Setting]
Alerter,4,"D:(A;OICI;GA;;;WD)"
Browser,4,"D:(A;OICI;GA;;;WD)"
Fax,4,"D:(A;OICI;GA;;;WD)"
cisvc,4,"D:(A;OICI;GA;;;WD)"
LicenseService,4,"D:(A;OICI;GA;;;WD)"
Messenger,4,"D:(A;OICI;GA;;;WD)"
RasAuto,4,"D:(A;OICI;GA;;;WD)"
RemoteAccess,4,"D:(A;OICI;GA;;;WD)"
TapiSrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWR
PWPDTLOCRSDRCWDWO;;;SY)"
Spooler,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;RPWPDTRC;;;
S-1-5-21-347615555-2441251375-4083693081-
1103)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
AppMgmt,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSW
RPWPDTLOCRSDRCWDWO;;;SY)"
wuauserv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSW
RPWPDTLOCRSDRCWDWO;;;SY)"
BITS,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPW
PDTLOCRSDRCWDWO;;;SY)"
ClipSrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRP
WPDTLOCRSDRCWDWO;;;SY)"
Browser,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWR
PWPDTLOCRSDRCWDWO;;;SY)"
DHCPServer,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLC
SWRPWPDTLOCRSDRCWDWO;;;SY)"
TlntSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRP
WPDTLOCRSDRCWDWO;;;SY)"
TapiSrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWR
PWPDTLOCRSDRCWDWO;;;SY)"
TermService,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLC
SWRPWPDTLOCRSDRCWDWO;;;SY)"

LicenseService,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
Messenger,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
mnmsrvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
Fax,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
NtLmSsp,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
RemoteAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
RemoteRegistry,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"

Appendix B:

Registry Permissions Table

Registry Key	User Groups	Permissions	Inherit Method
Classes Root	Administrators Creator Owner Systems Users	Full Control Full Control (subkeys only) Full Control Read	Replace
\Machine\Software	Administrators Creator Owner Systems Users	Full Control Full Control (subkeys only) 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
\Macnhine\Software\Microsoft\Protected Storage System Provider	Ignore		Ignore
\Machine\Software\Microsoft\Windows NT\CurrentVersion\AsrCommands *note: if not using the backup operators group, remove it from the permissions	Administrators Backup Operators*	Full Control Query, Set Value, Create Subkey, Enumerate, Notify, Delete, Read permissions	Replace

	Creator Owner System Users	Full Control (subkeys only) Full Control Read	
\Machine\Software\Microsoft\Windows NT\CurrentVersion\Perflib	Administrators Interactive Creator Owner System	Full Control Read Full Control Full Control	Replace
\Machine\Software\Microsoft\Windows\ CurrentVersion\GroupPolicy	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\ CurrentVersions\Policies	Administrators Authenticated Users Systems	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		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 System Users	Full Control Full Control (subkeys only) Full Control Read	Propagate
\Machine\System\controlset004	Administrators Creator Owner System Users	Full Control Full Control (subkeys only) Full Control Read	Propagate
\Machine\System\controlset005	Administrators Creator Owner	Full Control Full Control (subkeys only)	Propagate

	System Users	Full Control Read	
\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 *note: if not using the Backup operators group, remove the group from the permissions	Administrators 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		Ignore
\Machine\System\CurrentControlSet\HardwareProfiles	Administrators Creator Owner System User	Full Control Full Control (subkeys only) Full Control Read	Replace
\Machine\System\CurrentControlSet\Services\SNMP\Parameters\Permitted Managers	Administrators Creator Owner System	Full Control Full Control Full Control	Replace

\Machine\System\CurrentControlSet\ Services\SNMP\Parameters\ Valid Communities	Administrators Creator Owner System	Full Control Full Control Full Control	Replace
Users\.Default	Administrators Users Creator Owner System	Full Control Read Full Control (subkeysonly) Full Control	Replace
Users\.Default\Software\Microsoft\ NetDDE	Administrators System	Full Control Full Control	Replace
Users\.Default\Software\Microsoft\ Protected Storage Systems Provider	Ignore		Ignore

Appendix C:

File Permissions Table as set by NSA (Before replacing the "users" group)

Folder or File	User Groups	Recommended Permissions	Inherit Method
%ProgramFiles%	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Replace
%ProgramFiles%\Resource Kit (servers & domain controllers) %ProgramFiles%\Resource Pro Kit (workstations)	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	Full Control Full Control	Propagate

	SYSTEM Users	(subfolders and files) Full Control Read, Execute	
%SystemDirector%\Group Policy	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control	Propagate
%SystemDirctory%\ias	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate
%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		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 Users	Full Control Full Control Read, Execute	Propagate
%SystemDirectory%\spool\Printers	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders & files) Full Control Traverse folder,	Replace

		Read attributes, Read extended attributes, Create files, Create folders (folder and subfolders)	
%SystemDrive%	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (sub folders 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\Dr.Watson	Administrators CREATOR OWNER SYSTEM Users Users	Full Control Full Control (sub folders and files) Full Control Travers folder, Create files, Create folders (subfolders and files Read, Execute	Replace
%SystemDrive%\Documents and Settings\All Users\Documents\Dr.Watson\drwtsn32.log	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control Full Control Modify	Replace
%SystemDrive%\Inetpub (servers only)	Ignore		Ignore
%SystemDrive%\io.sys	Administrators	Full Control	Replace

	SYSTEM Users	Full Control Read, Execute	
%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 (sub folders and files) Full Control Read, Write, Execute	Replace
%SystemDrive%\System Volume Information	Ignore		Ignore
%SystemDrive%\Temp	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (sub folders and files) Full Control Traverse folder, Create files, Create folders (folders and subfolders)	Replace
%SystemRoot%	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (sub folders and files) Full Control Read, Execute	Replace
%SystemRoot%\$NtServicePack Uninstall$	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 (sub folders and files) Full Control Read, Execute	Propagate
%SystemRoot%\debug\UserMode	Administrators SYSTEM Users	Full Control Full Control Traverse Folder, List folder, Creat files (folder only)	Propagate

	Users	Create files, Create folders (files only)	
%SystemRoot%\NTDS (Domain Controllers only)	Administrators SYSTEM	Full Control Full Control	Propagate
%SystemRoot%\security	Administrators CREATOR OWNER SYSTEM	Full Control Full Control (sub folders and files) Full Control	Replace
%SystemRoot%\SYSVOL	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control (sub folders and files) Full Control	Propagate
%SystemRoot%\SYSVOL\domain\Policies	Administrators Authenticated Users CREATOR OWNER Group Policy Creator Owners SYSTEM	Full Control Read, Execute Full Control (sub Folders and files) Modify Full Control	Propagate
%SystemRoot%\Offline Web Pages	Ignore		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		Ignore
%SystemRoot%\Temp	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (sub folders and files) Full Control Traverse folder, Create files, Create folders (folders and subfolders	Replace
c:\ntbootdd.sys	Administrators SYSTEM	Full Control Full Control	Replace

File systems table after being modified for our environment (i.e.removing the users group and replacing it with branch managers)

Folder or File	User Groups	Recommended Permissions	Inherit Method
%ProgramFiles%	Administrators CREATOR OWNER SYSTEM Branch managers	Full Control Full Control (subfolders and files) Full Control Read, Execute	Replace
%ProgramFiles%\Resource Kit (servers & domain controllers) %ProgramFiles%\Resource Pro Kit (workstations)	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%	Administrators CREATOR OWNER SYSTEM Branch managers	Full Control Full Control (subfolders and files) Full Control Read, Execute	Replace
%SystemDirectory%\appmgmt	Administrators SYSTEM Branch managers	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 Branch managers	Full Control Full Control (subfolders and files) Full Control Read, Execute	Propagate
%SystemDirector%\Group Policy	Administrators Authenticated Users Branch managers SYSTEM	Full Control Read, Execute Full Control	Propagate
%SystemDirctory%\ias	Administrators SYSTEM Branch managers	Full Control Full Control Read, Execute	Propagate
%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		Ignore
%SystemDirectory%\repl	Administrators SYSTEM Branch managers	Full Control Full Control Read, Execute	Propagate
%SystemDirectory%\repl\export	Administrators Replicator SYSTEM Branch managers	Full Control Read, Execute Full Control Read, Execute	Propagate
%SystemDirectory%\repl\import	Administrators Replicator SYSTEM Branch managers	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 Branch managers	Full Control Full Control Read, Execute	Propagate
%SystemDirectory%\spool\Printers	Administrators CREATOR OWNER SYSTEM Branch managers	Full Control Full Control (subfolders & files) Full Control Traverse folder, Read attributes, Read extended attributes, Create files, Create folders (folder and subfolders)	Replace
%SystemDrive%	Administrators CREATOR OWNER SYSTEM Branch managers	Full Control Full Control (sub folders and files) Full Control Read, Execute	Propagate
%SystemDrive%\autoexec.bat c:\autoexec.bat	Administrators SYSTEM Branch managers	Full Control Full Control Read, Execute	Replace
%SystemDrive%\boot.ini	Administrators	Full Control	Replace

c:\boot.ini	SYSTEM	Full Control	
%SystemDrive%\config.sys c:\config.sys	Administrators SYSTEM Branch managers	Full Control Full Control Read, Execute	Replace
%SystemDrive%\Documents and Settings	Administrators SYSTEM Branch managers	Full Control Full Control Read, Execute	Propagate
%SystemDrive%\Documents and Settings\Administrator	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\Documents and Settings\All Branch managers	Administrators SYSTEM Branch managers	Full Control Full Control Read, Execute	Propagate
%SystemDrive%\Documents and Settings\Default User	Administrators SYSTEM Branch managers	Full Control Full Control Read, Execute	Replace
%SystemDrive%\Documents and Settings\All Branch managers\Documents\Dr.Watson	Administrators CREATOR OWNER SYSTEM Branch managers Branch managers	Full Control Full Control (sub folders and files) Full Control Travers folder, Create files, Create folders (subfolders and files Read, Execute	Replace
%SystemDrive%\Documents and Settings\All Branch managers\Documents\Dr.Watson \drwtsn32.log	Administrators CREATOR OWNER SYSTEM Branch managers	Full Control Full Control Full Control Modify	Replace
%SystemDrive%\lnetpub (servers only)	Ignore		Ignore
%SystemDrive%\io.sys	Administrators SYSTEM Branch managers	Full Control Full Control Read, Execute	Replace
%SystemDrive%\msdos.sys	Administrators SYSTEM Branch managers	Full Control Full Control Read, Execute	Replace
%SystemDrive%\My Download Files	Administrators CREATOR OWNER SYSTEM Branch managers	Full Control Full Control (sub folders and files) Full Control Read, Write, Execute	Replace
%SystemDrive%\System Volume Information	Ignore		Ignore
%SystemDrive%\Temp	Administrators CREATOR OWNER	Full Control Full Control (sub	Replace

	SYSTEM Branch managers	folders and files) Full Control Traverse folder, Create files, Create folders (folders and subfolders)	
%SystemRoot%	Administrators CREATOR OWNER SYSTEM Branch managers	Full Control Full Control (sub folders 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 Branch managers	Full Control Full Control (sub folders and files) Full Control Read, Execute	Propagate
%SystemRoot%\debug\UserMode	Administrators SYSTEM Branch managers Branch managers	Full Control Full Control Traverse Folder, List folder, Creat files (folder only) Create files, Create folders (files only)	Propagate
%SystemRoot%\NTDS (Domain Controllers only)	Administrators SYSTEM	Full Control Full Control	Propagate
%SystemRoot%\security	Administrators CREATOR OWNER SYSTEM	Full Control Full Control (sub folders and files) Full Control	Replace
%SystemRoot%\SYSVOL	Administrators Authenticated Users Branch managers CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control (sub folders and files) Full Control	Propagate
%SystemRoot%\SYSVOL\doma	Administrators	Full Control	Propagate

in\Policies	Authenticated Users Branch managers CREATOR OWNER Group Policy Creator Owners SYSTEM	Read, Execute Full Control (sub Folders and files) Modify Full Control	
%SystemRoot%\Offline Web Pages	Ignore		Ignore
%SystemRoot%\regedit.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\Registration	Administrators SYSTEM Branch managers	Full Control Full Control Read	Propagate
%SystemRoot%\repair	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\Tasks	Ignore		Ignore
%SystemRoot%\Temp	Administrators CREATOR OWNER SYSTEM Branch managers	Full Control Full Control (sub folders and files) Full Control Traverse folder, Create files, Create folders (folders and subfolders	Replace
c:\ntbootdd.sys	Administrators SYSTEM	Full Control Full Control	Replace

Last Updated: October 22nd, 2017

Upcoming Training

SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
Univ. of California - SEC505: Securing Windows and PowerShell Automation	**Los Angeles, CA**	**Jan 29, 2018 - Feb 03, 2018**	**vLive**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
Southern California- Anaheim 2018 - SEC505: Securing Windows and PowerShell Automation	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**vLive**
SANS 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS Security West 2018	**San Diego, CA**	**May 11, 2018 - May 18, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**