Global Information Assurance Certification Paper

GIAC Certified Windows Security Administrator (GCWN)
Practical Assignment 3.1

Option 2: Securing Windows 2000 with Security Templates

Prepared by Bryce Thompson
April 2003

Table of Contents

Summary
Mass-adoption of networking technology and the Internet has allowed organizations to greatly increase their productivity. However, these great strides in communication have naturally caused information security to become more and more of a concern in the business arena. When Windows NT 4.0 was released in 1996, it offered many security enhancements over the other products in the Windows family. More support for hardening the OS has been enabled over the years in the form of Service Packs and hotfixes. However, in many cases the default OS configuration was not as secure as some organizations required. Microsoft offered security checklists for different server and workstation roles, which was helpful in assisting administrators with the many choices that needed to be made. Nevertheless, the act of securing a Windows NT 4.0 system was a manual process with many drawbacks and limitations:

- Several different tools were needed for proper security configuration, such as Windows Explorer, User Manager, and the Registry Editor.
- Some security configuration settings in the Registry could be automated through the application of a Registry file. However, a great deal of Windows NT security configuration was very complex and time-consuming, such as the setting of permissions on the file system and Registry keys.
- There was no way to ensure that settings hadn't been changed without the use of 3rd party tools. In addition, any settings that had been changed would likely need to be re-configured manually.
- Most importantly, manual security configuration lends itself to human error. Over time, this results in a non-standard environment which becomes increasingly difficult to secure and troubleshoot.

Microsoft's first foray into providing a unified GUI for the application and automation of security settings was the Security Configuration Editor (SCE) in Windows NT 4.0 Service Pack 4. This functionality is built into Windows 2000 and may be accessed through the Security Template and Security Configuration and Analysis (SCA) snap-ins for the MMC. In Windows 2000, the GUI can be used to bundle security settings together into an .inf file known as a security template. Once a security template has been designed for the needs of an organization, it can be used to assign security parameters to systems throughout the enterprise. The following real-world scenario chronicles how a security template has been leveraged to secure Windows 2000 print servers at Midwest Bank, a fictional organization that has not yet been able to migrate to Active Directory. This paper provides an in-depth analysis of Midwest Bank's selection of an existing security template, the modification of this template to suit the needs of the organization, and a discussion of their template testing and evaluation process. I will explore the ways in which Midwest Bank's print server security template allows automation and consistency of security settings, provides the flexibility needed in order to maintain connectivity to their current Windows NT 4.0 domain environment, and assists the organization in preparing for their future Active Directory migration.

1. Introduction

Midwest Bank is a fictional financial institution based in Chicago, Illinois. It was chartered in the mid-1960s, and has aggressively expanded through the years. In the 1970s and 1980s, the organization focused on acquisitions of several small community and farmer's banks. However, in the late 1990s they merged with two regional banks in Indiana and Michigan. The resulting organization is now truly an institution that lives up to its name, with 2,000 users in 100 branches scattered across the Midwest. Besides the branch users, 500 corporate users reside at the central office in Chicago, 300 in the old home office of the Bank of Indiana in Indianapolis, and 400 in the old home office of Michigan Federal in Detroit, Michigan. This has resulted in the server environment described below. All servers are running Windows NT 4.0 on Service Pack 6a with the Security Rollup package and all security hotfixes since July 2001. Other technologies outside the NT domain model, such as mainframe connectivity, are outside the scope of this document.

Classification	Technology in use
Domain controllers and structure	Three Windows NT domains (MIDWEST, INDYBANK, and MFEDERAL. Windows NT PDCs reside in the central offices in Illinois, Michigan, and Indiana. BDCs are scattered in a few strategic locations across the enterprise.
Core networking services	Windows NT DHCP, DNS, and WINS.
Web servers	IIS for internal communication—Internet web hosting is outsourced.
E-mail servers	Lotus Notes (Domino 5.10)
Software distribution	SMS 2.0
Backup software	Veritas BackupExec 8.6
Database servers	Microsoft SQL Server 7.0
Security products	Norton AntiVirus 7.5 CE, Symantec Intruder Alert 3.6, and Bindview bv-control.

Table 1

After the second (and larger) merger with Michigan Federal, integration of customer service systems, teller operations, and mainframe financial processing systems became management's main concern. Domain and server consolidation was simply a lower priority. Luckily the three banks' systems were compatible in many respects when it came to domain and server OS operability—all three were Microsoft shops to a great extent. They were on Windows NT 4.0 domains, used NT 4.0 application servers, used Lotus Notes as their corporate e-mail standard, and so on. Other than some upgrades to SQL Server 7.0 from 6.5, the environments were very similar. In order to save time, the three domains were simply connected together with two-way trust relationships. This worked well enough at first, while operations were still relatively separate between the three institutions.

However, after more time passed between the mergers, more consolidation of operations at Midwest Bank's home office was necessary. In addition,

supporting and maintaining the three Windows NT 4.0 domains became both time-consuming and complex. Granting access to resources across domains as users moved across the enterprise became very difficult to administer and troubleshoot. In addition, the trust relationships were becoming unreliable at times. Even with only three domains, production outages have in the past caused the secure channel between the domains to fail. These problems needed to be solved, because management wasn't expected to close the offices of the merged banks in Indiana and Michigan anytime in the foreseeable future. It became obvious that the scalability problems of the three Windows NT domains were costing more money to maintain, and were keeping the new organization from realizing the benefits of the merger.

A Windows 2000 transition team was formed between the IT groups in Midwest Bank, Bank of Indiana, and Michigan Federal. Project managers, Audit, Information Security, server administrators, and end-user support personnel were all represented. They were charged with developing standards and procedures for use in the future for all Windows 2000 servers. The server administrators on the team specialized in building the Windows 2000 servers and customizing them for the enterprise. They developed an unattended Windows 2000 Advanced Server install that would serve as the basis for all Windows 2000 servers in the Midwest Bank environment. The unattended install was network-based, from a file server that serves as a distribution point, to ensure that the installation could be quickly and easily updated. In order to protect the unattended installation files on the distribution point, the staging area was located on a separate, closely monitored pre-production network that only served as a connection point to run the unattended install procedure. The unattended install was slipstreamed with Service Pack 3, and did not install any games or elements of IIS. The unattended install used cmdlines.txt to run a batch file during Windows 2000 Setup, which is responsible for deploying all relevant hotfixes that needed to be installed on top of SP3. As of the time of this writing, these hotfixes were as follows:

MS03-004: Cumulative Patch for Internet Explorer (Q810847)
MS03-001: Unchecked Buffer in Locator Service Could Lead to Code Execution (Q810833)
MS02-071: Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation (Q328310)
MS02-070: Flaw in SMB Signing Could Enable Group Policy to be Modified (Q329170)
MS02-069: Flaw in Microsoft VM Could Enable System Compromise (Q810030)
MS02-065: Buffer Overrun in MDAC Could Lead to Code Execution (Q329414)
MS02-055: Unchecked Buffer in Windows Help Facility Could Enable Code Execution (Q323255)
MS02-050: Certificate Validation Flaw Could Enable Identity Spoofing (Q329115)
MS02-048: Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates (Q323172)

MS02-045: Unchecked Buffer in Network Share Provider can lead to Denial of Service (Q326830)
MS02-042: Flaw in Network Connection Manager Could Enabled Privilege Elevation (Q326886)

1.1 Description of the future Windows 2000 environment

The long-term direction for Midwest Bank's central IT group is to migrate the Windows NT 4.0 domains to a single Active Directory domain in native mode, which will provide the organizational structure and reliable replication services that are needed to consolidate operations at Midwest Bank. Administrators also want the granularity of administrative rights and delegation of control that an Active Directory domain will provide. The first stage of the Windows 2000 migration has already occurred with the migration of all workstations to Windows 2000 Professional. Since client applications needed to be standardized across the enterprise, the desktop team took the opportunity to roll out Windows 2000 workstations with application versions that were compatible with the new OS. In the second stage of the migration, all Windows NT servers across the enterprise will need to be replaced with Windows 2000 servers. The only exceptions are the domain controllers and core networking services (DHCP, DNS, and WINS), which will remain on Windows NT until the move to Active Directory. As the migration to Active Directory is the end goal, all Windows 2000 research and development will be conducted with Active Directory in mind.

The Windows 2000 transition team decided that print services was the easiest and least risky start for the Windows 2000 server migration path. Windows NT-based printing was well known and doesn't involve the migration of data. In addition, once the servers and printers were set up, users' logon scripts simply needed to point to the new Windows 2000 print servers. Administration of the new print servers would be roughly the same as Windows NT print servers. If results of the migration were not what was expected, the login scripts could just be changed back to reference the old Windows NT print servers until the issues have been resolved.

1.2 Description of the Windows 2000 print servers

The new Windows 2000 print servers were configured in a similar manner as the existing Windows NT 4.0 print servers. The installed clients on the Windows 2000 print server were Norton AntiVirus 7.5 Corporate Edition (for anti-virus protection), the SMS 2.0 client (for software distribution), Symantec Intruder Alert 3.6 (for security policy propagation), and Dell's OpenManage Server Assistant software (for hardware-based monitoring). The print server hardware was standardized on 1U Dell PowerEdge 1550s with 1 GB of RAM and three 36GB SCSI drives that were configured in a RAID 5 array. The OS resided on an 8GB C drive, the D drive was 8GB, and the remainder of the array was drive E. In Midwest Bank's environment, drive E was strictly used for the print spooler. All

production servers are behind three cardkey access points: one to get on the floor that houses the central IT area, one to access the data center, and one to access the production server racks. The production servers are racked inside a glass enclosure that is monitored 24 hours a day by security cameras and members of the Operations staff. The name for the first print server being built was A1PRINT01, and it would reside on the MIDWEST domain. Once it was configured, A1PRINT01 would service all 25 printers on the east side of the Midwest Bank central office. A second print server would house the printers on the west side of the building. All users would have access to the printers on the print server. The Operations group has printer administrators currently in the Print Operators group for the NT print servers, and those people would also be administering the queues on the Windows 2000 print servers.

1.3 Print server security risks in the Midwest Bank environment

Management wanted servers in the Midwest Bank environment to be held to a high security standard. That having been said, the transition team agreed that Windows 2000 print servers were relatively low-risk compared with file servers, web servers, and application servers in the enterprise. All users have the capability to print to network printers in the Midwest Bank environment. The current Windows NT print servers do not handle confidential material, because these print jobs are either printed to personal printers or handled by mainframe printers that are not part of the domain security model. Specialty printers, such as professional-quality color laser printers, are only accessible by the Graphics department. The Windows 2000 print servers wouldn't hold confidential user data, and the only user data that would reside on the server is temporarily contained in the print spooler. Infrastructure servers are not exposed to the Internet, and Midwest Bank has invested heavily in well-protected firewall hardware.

Servers in the Midwest Bank environment are remotely monitored in a number of ways. Information Security uses Bindview's bv-control product to scan for a pre-defined list of security vulnerabilities. In addition, the servers are also well monitored for hardware and software anomalies. Print servers, in particular, are monitored closely because administering them is notoriously labor-intensive. In the experience of the server administrators currently running Windows NT for file and print services, file servers are generally rather stable. Sometimes users take up too much space on their shared drives, and pre-configured alerts notify the administrators. However, print servers are continually accessed all day by users' print jobs, and one large color print job can cause processing delays for all users with printers attached to the server. In addition, users quickly notice when their print server goes down. As a result, the members of the Operators group are vigilant in monitoring print servers. The transition team agreed that the print server role does not carry special risks of its own, but needs to be protected from the general risks that all servers in the environment face: the threat of

information-gathering through reconnaissance, compromise for the purposes of distributed attacks, and denial of service.

2. Selection of existing security template to modify

The Windows 2000 transition team's research on the subject of security templates showed that this new Windows 2000 feature could be used to greatly simplify and speed the application of security settings. The team decided that security templates would be developed for all server roles. Keeping the security risks in mind, the goals for the transition team's print server security template were as follows:

- Automated and consistent application of security settings
- No impact on functionality
- Increase security over that of existing Windows NT 4.0 servers, where possible

The transition team was most concerned with ensuring that security settings are applied across all servers in a consistent manner. They also wanted to make sure these actions could be performed quickly, so the pace of the migration process could be accelerated. They also wanted to take advantage of this opportunity to increase their print server's base security level and distribute higher-security settings that currently existed in the Windows NT 4.0 environment. At the same time, functionality could not be compromised under any circumstances. The security template for the Windows 2000 print servers would be the first security template in production.

Several members of the team had experience with securing Windows NT 4.0 and understood what security settings are necessary in their environment. They understood how to secure an NT server, but had less experience in using security templates. The transition team discovered through their research that mistakes made with improper use of a security template could be very difficult to reverse. "The setup security.inf file…can be used to reset most of their settings to their default…values [but] the only sure-fire way to restore a system to its earlier configuration is via a backup" (Haney, p. 20). As a result, instead of starting from scratch, the transition team started with another template and modified it to suit their needs.

2.1 Evaluation of Microsoft built-in security templates: securedc.inf and hisecdc.inf

The transition team first evaluated the Microsoft templates that come with Windows 2000 Server, but the built-in templates didn't match their security goals. Securedc.inf was nowhere near strong enough for their environment because it left too many parameters at insecure default settings. The hisecdc.inf was too strong in some areas and too weak in others. For example, auditing in the

hisecdc.inf security template was too extreme and some Windows 2000-only settings were enabled. However, no suggestions were made in the hisecdc.inf security template for DACLs on the file system and the Registry. The team also didn't feel particularly comfortable in starting with a template that was specifically designed to secure a domain controller.

2.2 Evaluation of Microsoft's Common Criteria server templates (CC_Baseline_W2K_Server.inf and CC_HiSec_W2K_Server.inf)

The team downloaded Microsoft's Common Criteria Security Configuration Guide. Two templates discussed in this document were evaluated: a baseline (minimum) Windows 2000 Server configuration for Common Criteria compliance named CC_Baseline_W2K_Server.inf, and a high-security Windows 2000 Server configuration named CC_HiSec_W2K_Server.inf. There had never been any directive that the print servers adhere to Common Criteria specifications. However, back when the security policies for Windows NT were in development, the Information Security staff at Midwest Bank had researched the steps that were necessary for CC certification. The thinking at the time had been that some of these steps could be leveraged in Midwest Bank's environment, where appropriate. However, there were so many changes that needed to be made that the effort was not seen as a good value for the amount of development time needed. Now that security templates existed that can automatically set up some of the necessary parameters, the team felt that those templates were worth evaluation. However, the team didn't feel this template would be a good start for their customized template. In many cases, the security settings were appropriate and these templates were certainly much more secure than the built-in Microsoft templates. However, some design choices were either too extreme or not quite appropriate. For example, both the templates disabled almost 40 services—many of which were core services that would make a very significant impact on the server's capabilities. Also, the templates and documentation were not geared toward the general hardening of a Windows 2000 server, but specifically designed to describe and achieve a system that would meet the Windows 2000 Common Criteria Security Target. Even though good documentation was provided, it was geared strictly toward how to make a system CC-compliant and not enough explanation was provided about why the settings were chosen or what they do. Since Common Criteria certification was not a goal of the project, these templates were finally deemed to be unsuitable. However, the transition team did use the documentation to further their understanding of the configuration settings that could be used in a security template. A select few parameters in the final version of their security template resulted from the team's evaluation of the Common Criteria documentation.

2.3 Evaluation of the National Security Administration's W2K Server.inf security template

The engineers then evaluated the W2K Server.inf template, which was downloaded from the National Security Administration's web site. Not surprisingly, the NSA security template was highly secure and made a lot of configuration changes. The team's consensus was that a number of changes needed to be made in order to customize the template appropriately for the Midwest Bank environment and to get the template working for Windows 2000 servers authenticating to Windows NT 4.0 domains. The evaluation of this template sparked a lot of debate within the group. There were two factions: some were worried that starting with W2K Server.inf was too high risk. This template could significantly impact the functionality of the print servers, with little gain. Also, the group's preliminary analysis suggested that it would be less work to tighten Microsoft's securedc.inf template rather that start with the NSA's template and loosen it appropriately.

2.4 Security template choice

After discussions between the members of the transition team, the group finally decided to start with the NSA's W2K Server.inf security template, for these reasons:

- The NSA has an excellent reputation in the security arena
- The NSA has worked with other groups to develop the security settings in their template
- The NSA is constantly reviewing their template—small changes have been made periodically since it was originally released in May 2001.
- The NSA's template is well documented in the NSA's companion publication "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set." Especially because of the NT domain interoperability requirements, the group needed highly technical and specific information to make the right decisions. A more documented template would help them make intelligent choices.
- Starting with a stronger template and loosening security as needed will be good for the overall security of the enterprise.
- It was successfully argued that the Windows 2000 print servers would likely be a security "lowest common denominator." It certainly would be prudent to apply a more paranoid security template to more sensitive servers, like the domain controllers. However, Midwest Bank's print servers probably would not need extreme security measures. It was hoped that the template the team developed for the print servers could also be used as a "base" template that established baseline security parameters. In other words, no server would be permitted on the network unless they had at least applied the base template. In the future, incremental templates could be created that will go on top of the base template and secure application servers like IIS and SQL, file servers, e-mail servers, and so on. Starting with a looser template may be easier and good enough if the end result is a print server. However, for the template to

be used in assigning baseline security, it would need to be as secure as possible.

As a result, the transition team used the NSA's W2K Server.inf template as a starting place to build a template for their print servers. They decided to name the resulting template "w2kbase.inf" because they intended to re-use it when configuring security for other server roles. For the rest of this scenario, the NSA's W2K Server.inf security template will be identified as the "NSA template." The transition team's w2kbase.inf security template will be identified as the "w2kbase template." Security settings will be compared between the two templates in Section 3 of this paper.

The Security Templates MMC snap-in makes it easy to modify properties of the template that are represented in the GUI, but the template must be modified by hand for parameters that aren't represented—such as adding Registry values. It is also often more convenient to edit the template by hand. As a result, I will explain how to directly edit a template in the following sections. The complete syntax of the NSA and w2kbase templates are listed in Appendices A and B. Since the w2kbase template is being used here for teaching, I have re-ordered the template syntax in conjunction with the order of the settings discussed in this paper. Spaces have also been added to the template so it is easier to read and follow.

4. Comparison of security settings between NSA/w2kbase

The Security Template and the Security Configuration and Analysis MMC snap-ins cannot be used to directly compare two security templates. However, the SCA snap-in is designed to compare a security template with settings that exist in a security database. To compare these two templates in a graphical format, I will demonstrate the use of the SCA snap-in to import the NSA template into a new security database called nsa.sdb. Then, I will use the SCA snap-in to compare the w2kbase template to the NSA security settings. In cases where the templates have the same settings, a table has been created to illustrate the values in both of them. This is a good opportunity to illustrate how to analyze a template and use the SCA to apply a template on a Windows 2000 machine. It is important to stress that in a real testing situation, only the evaluated template would need to be used to configure a machine—this operation is being performed here for demonstrative purposes only. The first step in this demonstration is to use the NSA template to create a new security database:

1. Open the MMC by typing mmc at the Run box, and select Add/Remove Snap-in under the Console menu.

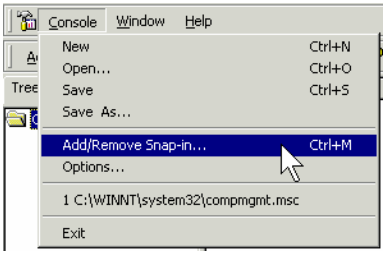

Figure 1

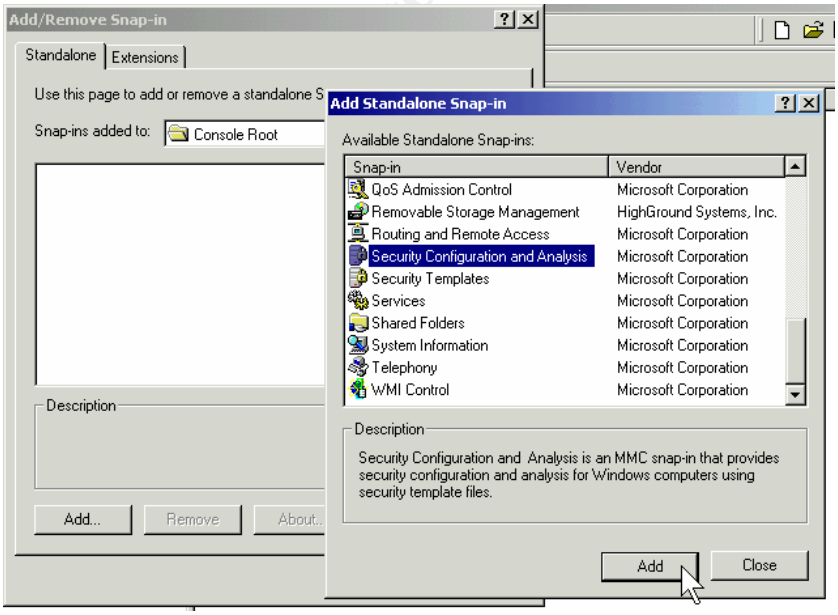

Figure 2

2. Right-click Security Configuration and Analysis and select Open Database.

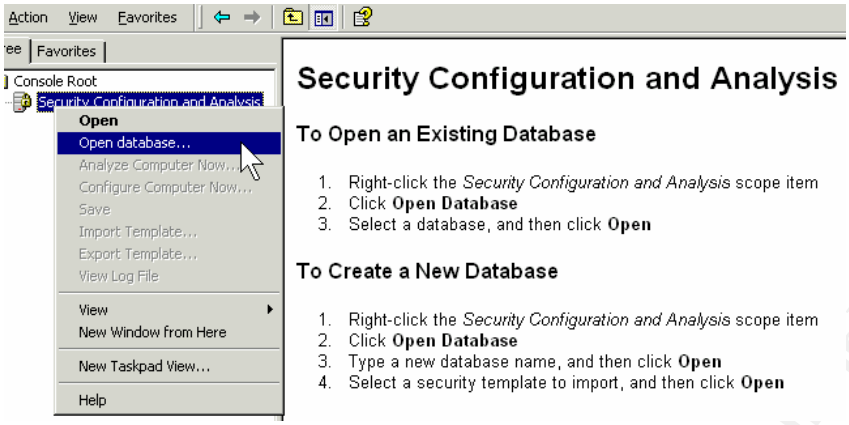

Figure 3

3. In the drop-down box, change the default location of C:\Documents and Settings\%username%\Local Settings\My Documents\Security to the location reserved by the OS for security databases: C:\Winnt\Security\Database. Do not delete, overwrite, or move the existing secedit.sdb security database, because this will negatively impact security template functionality.

4. Create a new security database by typing its name into the dialog box. Name the security database nsa.sdb and click Open.

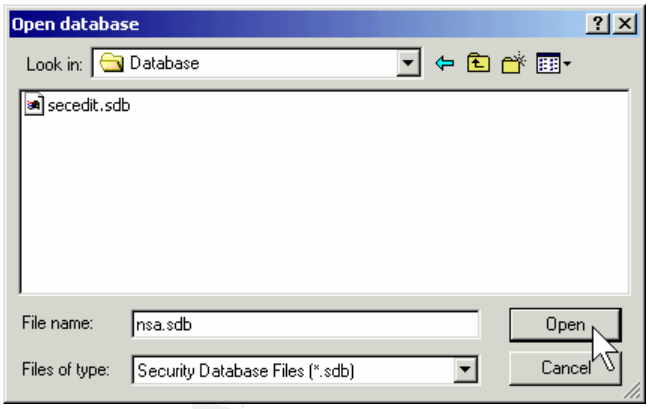

Figure 4

5. Since this is a new security database, a prompt will ask for the location of the security template to import into the new database. Select the NSA's W2K Server.inf template (continued on next page).

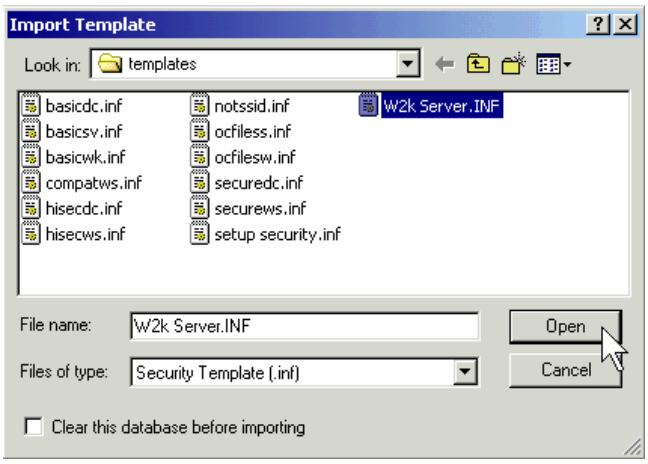

Figure 5

6. At this point, the new security database can be analyzed against the imported security template, or configured with it. Configure the computer with the settings in the NSA template by right-clicking Security Configuration and Analysis and selecting Configure Computer Now.

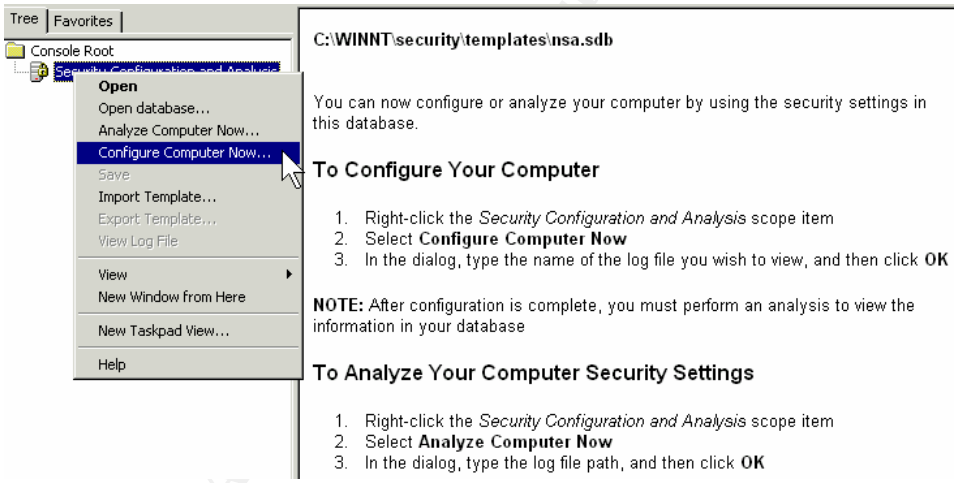

Figure 6

7. At the prompt for the name of the log file and the save location, name the file nsa.log. The file could be saved anywhere, but It is recommended to save the log file in C:\Winnt\Security\logs (continued on next page).

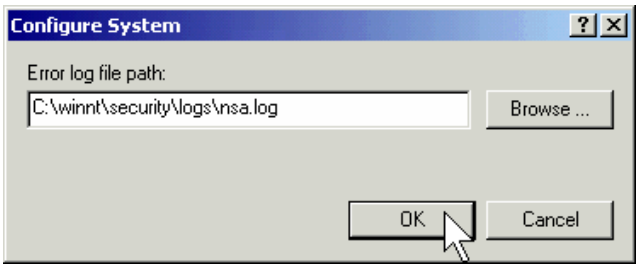

Figure 7

8. The computer has been configured with the security settings in the template. Use the SCA snap-in to compare the NSA-configured security database with the w2kbase.inf template by right-clicking Security Configuration and Analysis and selecting Import Template.

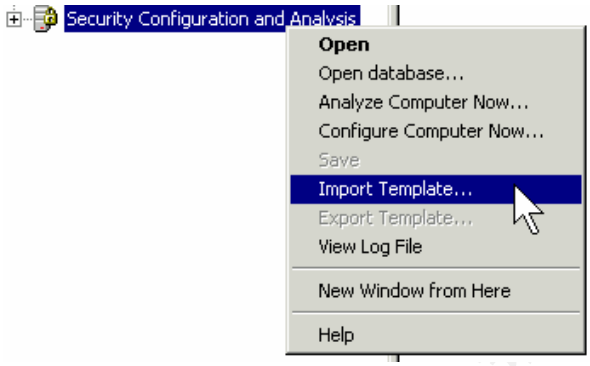

Figure 8

9. At the Import Template prompt, select w2kbase.inf and click Open.

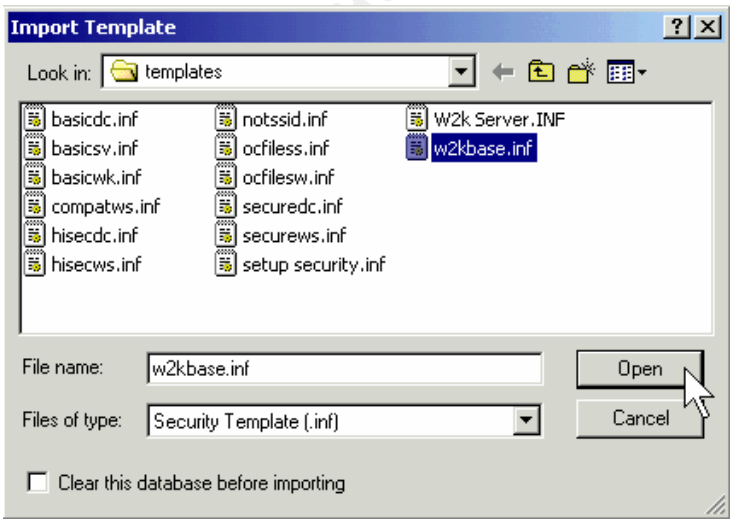

Figure 9

10. Start the analysis by right-clicking Security Configuration and Analysis and select Analyze Computer Now.

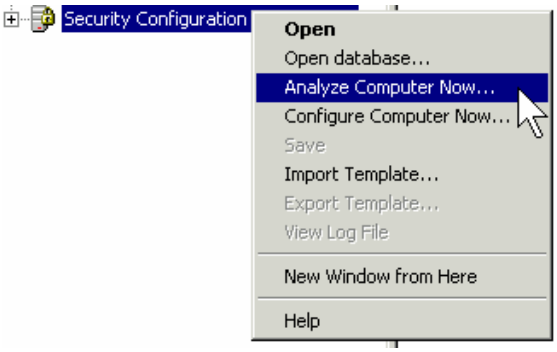

Figure 10

The result is a direct comparison between the two templates. In the following screen captures, the w2kbase template's settings are represented on the left under the "Database Setting" column. The NSA template's settings are on the right under the "Computer Settings" column. Settings that match are flagged with a green checkmark; settings that do not match are flagged with a red X. The templates are only checked for matches: there is no judgement that can determine whether a setting is more or less secure.

3.1 Account Policies\Password Policy

w2kbase = “Database Setting” values
NSA template = “Computer Setting” values

Policy	Database Setting	Computer Setting
Enforce password history	10 passwords remembered	24 passwords remembered
Maximum password age	31 days	90 days
Minimum password age	0 days	1 days
Minimum password length	8 characters	12 characters
Passwords must meet complexity requirements	Enabled	Enabled
Store password using reversible encryption for all users ...	Disabled	Disabled

Figure 11

Since the server being configured is not a domain controller, configuring password policy will not affect domain-based logons. Normally all logons will occur in the context of domain security, and the creation of local accounts on Windows 2000 member servers is forbidden in the Midwest Bank environment. However, the parameters for local accounts will still be set in the w2kbase template in accordance with Midwest Bank’s password policy. Some of the template values are stricter than the NSA’s recommendations, and some are looser. Midwest Bank’s password policy states that all passwords be at least eight characters long and expire after 31 days. Password filtering is enabled, which means that three out of four characters must be used: a lowercase letter, an uppercase letter, a number, and a special character. Users are not required to logon to change their passwords. The setting for Minimum Password Age is zero, which means that users can change their password at any time. This setting is in use at Midwest Bank because it is generally believed that allowing users to immediately change their passwords without administrative assistance encourages secure behavior on behalf of the user community. Passwords are remembered for ten months, so users are not likely to cycle around and re-use a favorite password. The Store Password using Reversible Encryption is only necessary when users are connecting to a 3rd party system that cannot access domain passwords unless they are stored using reversible encryption. Since reversible encryption is not much more secure than clear-text passwords, it is never recommended to enable this setting.

3.2 Account Policies\Account Lockout Policy

w2kbase = “Database Setting” values
NSA template = “Computer Setting” values

Policy	Database Setting	Computer Setting
Account lockout duration	0	15 minutes
Account lockout threshold	3 invalid logon attempts	3 invalid logon attempts
Reset account lockout counter after	99999 minutes	15 minutes

Figure 12

All of the settings here are as strong as or stronger than the NSA template, in accordance with Midwest Bank’s account lockout policy. Users have three tries before an account is locked out, and once it is locked out it will require an Administrator to unlock it. In Windows NT and 2000, the account lockout counter will automatically reset to zero after a preset amount of time. 99,999 minutes (or almost 28 days) is the maximum value for automatic reset of the account lockout counter. It cannot be entirely disabled, but setting the value to the maximum effectively stops an intruder.

3.3 Account Policies\Kerberos Policy

The NSA and w2kbase templates make no changes to Kerberos settings. As explained in the NSA documentation:

> Since Active Directory is necessary for Kerberos authentication, the Kerberos policy only has significance for the Windows 2000 domain Group Policy Object. Therefore, for the…server configurations that this document addresses, the Kerberos policies will not be defined" (Haney, p. 27).

As the w2kbase template is also not designed for a domain GPO, and since Kerberos cannot be used for authentication on a Windows NT 4.0 domain, the template also makes no changes to the defined settings. All of the settings under Kerberos Policy are left at "Not Defined." It is important to mention that a setting of "Not Defined" in a security template means that the template leaves any existing setting alone. Whether the setting is the Windows 2000 default value or was manually changed to something else, the template does not configure it in any way.

3.4 Local Policies\Audit Policy

By default, auditing is not enabled on Windows 2000 member servers. When auditing is configured, system access control lists (SACLs) control the generation of audit-related logging. More auditing is generally considered to be beneficial in the securing of a system, but auditing takes a toll on system performance. The processing spent on monitoring and logging audit events does leave the server with less resources for serving clients, so it is recommended that administrators not use auditing more than necessary. Except in special situations, Midwest Bank's administrators have done most of their auditing on the domain controllers and not done much local auditing on the NT servers. However, the transition team wants to enable more local auditing for better security. The transition team agrees with all of the NSA's auditing recommendations, because they feel these choices strike a good balance between security and functionality. Some of the audited events described here are intended for auditing on domain controllers, but the transition team has decided to include them in this template for later use. The chosen settings are discussed in the order of the table below.

Audit policy	Template setting
Account logon events	Success, Failure
Account management	Success, Failure
Directory service access	No Auditing
Logon events	Success, Failure
Object access	Failure
Policy change	Success, Failure
Privilege use	Failure
Process tracking	No auditing
System events	Success, Failure

Table 2

Auditing account logon events will capture logons and logoffs that occur at the domain level. When a user logs on or off with their domain account, it is an event logged by this setting. Normally a domain controller will have this setting enabled. Enabling it on a member server will have no effect, but the team decided there would be no harm doing so.

Auditing account management events will capture changes made in user accounts and groups. This includes account creation, deletion, modification, and any changes in group membership. The transition team wants all modifications in this area to be logged.

Auditing directory service events allows auditing of any property in Active Directory. As such, there is some overlap with account management auditing, except it has the potential for an extreme level of granularity. When Midwest Bank moves to Active Directory, likely they will be less concerned with auditing account management events and more concerned with deciding what properties of Active Directory that need to be audited. It is important to remember that the required Active Directory parameters for auditing must be set after this value is

enabled, much like auditing any other resource. Since Midwest Bank is not yet using Active Directory and has not yet discussed what needs to be audited or the necessary level of auditing, this has been set to No Auditing for now.

Auditing logon events will capture interactive and network-based logons/logoffs on the local machine. For the purposes of this template, this setting will be more important than the auditing of account logon events. Auditing both success and failure will capture any type of logon attempt. Since this logs both local and domain events, this setting will even log local Administrator account logon attempts.

Auditing object access enables resources auditing. Once this is set, Administrators must also select the objects that need to be audited. This includes files, folders, Registry keys, printers, and any other objects that can have a SACL assigned to them. The transition team has decided that auditing will not be generally necessary for successful access of a resource, so auditing will only be enabled for failure. This is in an attempt to keep log files to a minimum. Success auditing can cause the security log to quickly grow unmanageable, and administrators are more concerned with finding attempts at unauthorized access than wading through huge logs of authorized access. In general, printing in Midwest Bank's environment is not audited because all users can print to networked printers. In situations where success auditing needs to be enabled, this setting may be changed on a case-by-case basis.

Auditing policy changes will capture changes made to the audit policies themselves, as well as user rights assignments. The transition team feels this setting needs to be both success and failure.

Auditing privilege use will capture the exercising of user rights, such as changing the system time. A listing of all user rights can be found in section 3.5 (User Rights Assignment). It has been decided to audit failure only for the same reasons as object access—auditing successful access of user rights is not normally necessary and only causes the log files to grow.

Auditing process tracking will capture "program execution, process loading and unloading, file system handle creation and release, indirect object access, and other low-level OS behaviors like program execution and process loading and unloading." (Fossen, Group Policy, p. 109). This functionality is seldom enabled in any form because gathering the information is not normally worth the resulting impact on system performance. The transition team does not want this information to be captured on print servers.

Auditing system events will capture system-wide events, such as system startup and shutdown. It also records clearing of event logs. As a result, this information must be audited for both success and failure.

3.5 Local Policies\User Rights Assignment

Policy	Default OS setting	Template setting
Access this computer from the network	Backup Operators, Power Users, Users, Administrators, Everyone	Administrators, Users
Act as part of the OS	(None)	(None)
Add workstations to domain	(None)	(None)
Back up files and directories	Backup Operators, Administrators	Administrators
Bypass traverse checking	Backup Operators, Power Users, Users, Administrators, etc.	Users
Change the system time	Power Users, Administrators	Administrators
Create a pagefile	Administrators	Administrators
Create a token object	(None)	(None)
Create permanent shared objects	(None)	(None)
Debug programs	Administrators	(None)
Deny access to this computer from the network	(None)	(None)
Deny logon as a batch job	(None)	(None)
Deny logon as a service	(None)	(None)
Deny logon locally	(None)	(None)
Enable computer and user accounts to be trusted for delegation	(None)	(None)
Force shutdown from a remote system	Administrators	Administrators
Generate security audits	(None)	(None)
Increase quotas	Administrators	Administrators
Increase scheduling priority	Administrators	Administrators
Load and unload device drivers	Administrators	Administrators
Lock pages in memory	(None)	(None)
Log on as a batch job	(None)	(None)
Log on as a service	(None)	(None)
Log on locally	Backup Operators, Power Users, Users, Administrators, %computername%\Guest, %computername%\TsInternet…	Administrators
Manage auditing and security log	Administrators	Administrators
Modify firmware environment values	Administrators	Administrators
Profile single process	Power Users, Administrators	Administrators
Profile system performance	Administrators	Administrators
Remove computer from docking station	Power Users, Users, Administrators	(None)
Replace a process level token	(None)	(None)
Restore files and directories	Backup Operators, Administrators	Administrators
Shut down the system	Backup Operators, Power Users, Administrators	Administrators
Synchronize directory service data	(None)	(None)
Take ownership of files or other objects	Administrators	Administrators

Table 3

Domain user accounts also receive user rights from the domain, in accordance with the policies assigned at the domain level. Since practically all logons will occur in the context of domain security, the settings here will not normally impact users. One exception, however, is the local Administrator account. Because this account is locally defined, it will be restricted in accordance with the user rights above. Many of the values in this section of the template are already assigned by default. The changes made by the NSA and w2kbase templates mainly serve to restrict any users that might be members of the built-in Backup Operators and Power Users groups. Power Users and Backup Operators are not used in Midwest Bank's environment, so it is desirable to limit these groups. The user groups that can log on to the server, whether interactively or over the network, are also limited.

Even though the transition team accepted the NSA's recommendations concerning user rights, they did make some cosmetic changes in this area of the w2kbase template. In the NSA template, user rights are assigned with Security ID (SID) numbers. By default, this is what happens when the Security Templates GUI is used to build user rights into a security template. Using the GUI to assign user rights results in a lot of clicking, so the transition team put an extra section in the w2kbase template that translates SIDs into the groups they represent. This new section of the template was discovered in the CC_HiSec_W2K_Server.inf security template, but is not discussed in Microsoft's accompanying documentation (Science Applications International Corporation, p. F-35). This strings section is reprinted here:

```
[Strings]
SceInfAdministrator = Administrator
SceInfAdmins = Administrators
SceInfAcountOp = Account Operators
SceInfAuthUsers = Authenticated Users
SceInfBackupOp = Backup Operators
SceInfDomainAdmins = Domain Admins
SceInfDomainGuests = Domain Guests
SceInfDomainUsers = Domain Users
SceInfEveryone = Everyone
SceInfGuests = Guests
SceInfGuest = Guest
SceInfPowerUsers = Power Users
SceInfPrintOp = Print Operators
SceInfReplicator = Replicator
SceInfServerOp = Server Operators
SceInfUsers = Users
```

The strings work the same way as SIDs do, except they are easier to manage. For example, the syntax for assigning backup rights between the two templates is as follows:

NSA template syntax	w2kbase template syntax
sebackupprivilege = *S-1-5-32-544	sebackupprivilege = %SceInfAdmins%

Table 4

This assists in template management because it becomes easier to edit the template by hand. Administrators don't have to consult the list of well-known SIDs if they need to make modifications. Also, it may be easier for administrators to notice any inappropriate entries in the template when these string values are used. The string values can also be re-used when configuring Restricted Groups, as will be shown in Section 3.9

3.6 Local Policies\Security Options:

w2kbase = “Database Setting” values
NSA template = “Computer Setting” values

Policy	Database Setting	Computer Setting
Additional restrictions for anonymous connections	Do not allow enumeration of SAM accounts a...	No access without explicit anonymous permissions
Allow server operators to schedule tasks (domain...	Not defined	Not defined
Allow system to be shut down without having to l...	Disabled	Disabled
Allowed to eject removable NTFS media	Administrators	Administrators
Amount of idle time required before disconnectin...	15 minutes	30 minutes
Audit the access of global system objects	Disabled	Enabled
Audit use of Backup and Restore privilege	Disabled	Enabled
Automatically log off users when logon time expir...	Enabled	Enabled
Clear virtual memory pagefile when system shuts...	Disabled	Enabled
Digitally sign client communication (always)	Disabled	Disabled
Digitally sign client communication (when possible)	Enabled	Enabled
Digitally sign server communication (always)	Disabled	Disabled
Digitally sign server communication (when possible)	Enabled	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled	Disabled
Do not display last user name in logon screen	Enabled	Enabled
LAN Manager Authentication Level	Send NTLMv2 response only\refuse LM & NTLM	Send NTLMv2 response only\refuse LM & NTLM
Message text for users attempting to log on	This computer,its software including,without l...	
Message title for users attempting to log on	Press Ctrl+Alt+Del to Login	
Number of previous logons to cache (in case dom...	0 logons	0 logons
Prevent system maintenance of computer accoun...	Disabled	Disabled
Prevent users from installing printer drivers	Disabled	Enabled
Prompt user to change password before expiration	14 days	14 days
Recovery Console: Allow automatic administrativ...	Disabled	Disabled
Recovery Console: Allow floppy copy and access ...	Enabled	Disabled
Rename administrator account	a1hjs77	Administrator
Rename guest account	Adminstrator	Guest
Restrict CD-ROM access to locally logged-on user...	Enabled	Enabled
Restrict floppy access to locally logged-on user only	Enabled	Enabled
Secure channel: Digitally encrypt or sign secure c...	Disabled	Disabled
Secure channel: Digitally encrypt secure channel ...	Enabled	Enabled
Secure channel: Digitally sign secure channel dat...	Enabled	Enabled
Secure channel: Require strong (Windows 2000 o...	Disabled	Disabled
Send unencrypted password to connect to third-...	Disabled	Disabled
Shut down system immediately if unable to log se...	Disabled	Enabled
Smart card removal behavior	Lock Workstation	Lock Workstation
Strengthen default permissions of global system ...	Enabled	Enabled
Unsigned driver installation behavior	Warn but allow installation	Warn but allow installation
Unsigned non-driver installation behavior	Silently succeed	Warn but allow installation

Figure 13

All of these settings are found somewhere in the Registry, but the template provides an easy, more reliable way to change the values. Because there are some significant changes made to the NSA template in this area, the values will be addressed in groups of like settings:

Logon and authentication configuration

3.6.1 The “additional restrictions for anonymous connections” value in the GUI is also known as the RestrictAnonymous value in Windows NT 4.0, and it is located in the Registry in HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Restrict Anonymous. For years, Windows NT 4.0 administrators have enabled the setting of 1, which translates to “Do not allow enumeration of SAM accounts and

shares." This setting make it more difficult for account information to be extracted through an unauthenticated (null) session. In Windows 2000, a new value of 2 is supported, which translates in the GUI to "No access without explicit anonymous permissions." This actually "removes the SID of the Everyone group from the Security Access Token (SAT)" of the Anonymous Users group (Fossen Group Policy, p. 103). Since null session attacks have been discovered which get around the protections of value 1, the NSA recommends that organizations use the value of 2 if possible. If necessary for permissions to be assigned to anonymous users, perhaps for legacy application compatibility, these permissions would need to be assigned to the Anonymous Logon group.

However, using "no access without explicit anonymous permissions" is not supported for users logging onto a Windows NT 4.0 domain. This is because Windows NT uses null sessions in the process of logging a user onto the system. If this setting were set to the NSA's recommended value, users would no longer be able to log onto the NT 4.0 domain. In fact, even after the entire domain has moved to Active Directory and switched to Native Mode, all server applications will need to be stringently tested to ensure their compatibility with the loss of anonymous enumeration. It is important to mention that null sessions are not to be confused with the IUSR_*computername* account, which grants anonymous access to web content on IIS. This account is not affected by restricting null sessions.

3.6.2 "Allow system to be shut down without having to log on" is disabled by default for systems with some version of the Windows NT/2000 Server OS installed. This setting is not changed by either template. However, it is important to remember that an administrator can still remotely shut down the machine if they have the right to do so, even if no one is currently logged on. Windows 2000 will still gracefully shut down if the power button is pressed, and of course the machine will power off if the power cables are physically removed from the system. A combination of physical access control and auditing is required to help protect a system from unauthorized shutdown, or at least ascertain who performed the unauthorized action.

3.6.3 "Amount of idle time required before disconnecting session" refers to Microsoft Networking sessions. For example, if a user maps a drive to an NT/2000 file server but stops actively using the share, the user is disconnected after the allotted time period. However, when the user tries to use the share again, they are automatically re-connected. The default time for session disconnect is 15 minutes, and the transition team feels it is important to leave this setting at the default value even though the NSA template increases the value to 30 minutes.

3.6.4 "Automatically log off users when logon time expires" refers to the use of logon hours. Enabling this setting results in a user being automatically logged off when their logon hours expire. Logon hours are not in use at Midwest Bank, but

the transition team sees no reason not to accept the NSA's recommendation—if logon hours are ever instituted at Midwest Bank, an appropriate setting will already be in use.

Note: the parameters below that reference encryption/signing of client and server communications refer to SMB communication. Windows 2000 and Windows NT with Service Pack 4 or greater support SMB signing and encryption, which keep a "man-in-the-middle" attack from eavesdropping on or modifying SMB communications between a client and a server. Enabling signing protects against a third party tampering with the information, while encryption scrambles the packets and only allows the two computers participating in the SMB session to communicate. Midwest Bank does not currently use SMB signing because of some incompatibilities they encountered with Windows 2000 clients on a Windows NT 4.0 domain. They intend to use IPSec for encrypting all TCP/IP traffic once they move to Active Directory, thereby protecting more than just SMB sessions.

3.6.5 "Digitally sign client communication (always)" requires a client to use SMB signing. In addition, the client will refuse SMB communications with a server that doesn't support SMB signing. This requires all SMB servers in the enterprise to support SMB signing. As a result, the NSA recommends disabling this setting, and the transition team has also disabled it in their template.

3.6.6 "Digitally sign client communication (when possible)" directs a client to use SMB signing. However, if a server doesn't support SMB signing, the client will fall back to an older version of the SMB protocol that doesn't support SMB signing. In case Midwest Bank decides to use SMB signing at a later date, they have accepted the NSA recommendation and enabled SMB signing for clients when possible.

3.6.7 "Digitally sign server communication (always)" requires the server to use SMB signing. In addition, the server will refuse SMB communications with a client that doesn't support SMB signing. This requires all SMB clients in the enterprise to support SMB signing. As a result, the NSA recommends disabling this setting, and the transition team has also disabled it in their template.

3.6.8 "Digitally sign server communication (when possible)" directs the server to use SMB signing. However, if a client doesn't support SMB signing, the server will fall back to an older version of the SMB protocol that doesn't support SMB signing. In case Midwest Bank decides to use SMB signing at a later date, they have accepted the NSA recommendation and enabled SMB signing for servers when possible.

3.6.9 Disabling the "Disable CTRL+ALT+DEL requirement for logon" actually turns on the requirement for pressing Ctrl+Alt+Del to log onto a machine. This is the default when any Windows 2000 computer has been joined to a domain, even if it had not been the default before being joined. This setting will not be

changed.

3.6.10 Enabling the “Do not display last user name in logon screen” simply removes the last logged-in user name from the logon prompt. It is recommended so an attacker cannot use the last logged-on account as a known target.

3.6.11 “LAN Manager authentication level” is known in Windows NT 4.0 as the “LMCompatibilityLevel,” and it is found in the Registry under HKLM\SYSTEM\CurrentControlSet\Control\Lsa. This setting is used to configure the authentication protocols accepted by the system. Systems will use the weakest agreed authentication protocol permitted by both systems, so it is possible that a machine set to the default value can be attacked using LM even if it normally uses NTLM. LAN Manager, also known as LM, is a weak authentication protocol that is only included for compatibility purposes with Windows 95 and 98. Since only Windows NT 4.0 and Windows 2000 are in use at Midwest Bank, LM authentication can be safely disabled. NT LAN Manager, also known as NTLM, is a stronger authentication protocol that has been in use at Midwest Bank for quite some time. However, a newer form of the NTLM protocol is supported by default on Windows 2000 and NT 4.0 machines that have had Service Pack 4 installed. NTLM v2 is the best choice because it is much more difficult to crack an NTLMv2 password hash. Unlike NTLMv2, LM and NTLMv1 do not “add random bytes to the hashing process…two identical passwords will yield identical hashes, hence, pre-computed dictionaries of hashes can be used to quickly crack the encryption.” (Fossen, Active Directory, p. 23). After verifying that Windows NT 4.0 with Service Pack 4 supports NTLM v2 by default without making changes to the domain controllers, they decide to take advantage of NTLM v2 and increase security. The transition team decided to accept the recommendation of the NSA and increase this setting to its maximum value.

3.6.12 “Message text” and “message title” customize the logon box for a legal message before the user logs on. It allows an organization to require the user to accept a message before they can log on. In Midwest Bank’s case, the message title is simply “Press Ctrl+Alt+Del to Login.” The message text that has been supplied by their Legal department is as follows:

“This computer, its software including, without limitation electronic mail, and information processed by this computer are the property of Midwest Bank, to be used solely for business purposes. Information accessed by, contained in, maintained on, or transmitted by this computer, including without limitation electronic mail, should not be considered to be personal or private. Midwest Bank reserves the right to monitor, access, view, and copy the contents of this computer at any time.” This is Midwest Bank’s standard legal disclaimer, which resides on all machines. The NSA does recommend using the logon banner for legal purposes and even prints the Department of Defense’s logon warning in Appendix A of their documentation as an example, but ultimately an organization

must develop their own.

3.6.13 “Number of previous logins to cache” refers to cached logon configuration. This is normally done to provide a backup authentication method when a domain controller is not available. Another popular use of cached logons is for laptops, so they don’t have to use one account on the domain and a local account when not connected to the domain. By default, Windows NT/2000 will cache up to ten logons. In the case of a Windows 2000 member server, cached logons would not be necessary or desired. In the case where the domain weren’t available, like if the network connection failed and the domain could not be contacted, an administrator would get the local Administrator password (located in firecall escrow in Midwest Bank’s environment) and log on locally for troubleshooting purposes. The transition team agrees with the NSA’s recommendation and sets this value to zero.

3.6.14 “Prevent system maintenance of computer accounts” prevents machines from automatically requesting a weekly password change on their domain computer accounts. Both templates accept the default setting of Enabled.

3.6.15 “Prompt user to change password before expiration” allows customization of the number of days before a user is automatically prompted to change their password. 14 days before expiration is the default, and neither template changes this value.

3.6.16 “Rename Administrator account” and “rename Guest account” simply change the names of these local accounts. The NSA’s template does not address this setting because it is so individual to an organization, but their documentation recommends that the account names be changed. This feature can be defeated by hackers that simply attack or try to place themselves in the well-known local Administrator group SID of S-1-5-32-544. However, it may fool those who simply type “Administrator” or have that value in a script. The Guest account is not thought of as a terribly attractive security target as it is disabled by default and does not have rights to do much on the system. However, renaming the account isn’t harmful because it is never used in Midwest Bank’s environment. In addition, it has purposely been misspelled because this could fool a hacker who has successfully enumerated all local users into believing that the Administrator account has not been renamed.

Note: When a computer on the domain boots up, its Netlogon service establishes a “secure channel” between the machine and its domain controller. Authentication is established between the two systems and sensitive communications, such as a password exchange, are encrypted. However, by default some information is not encrypted and the secure channel is not integrity checked. “On Windows NT, Service Pack 4 or later permits an administrator to increase the security of the NetLogon channel. With SP4, all NetLogon channel data can be encrypted and digitally signed for integrity (Fossen, Active Directory,

p. 93). The values that follow configure the secure channel.

3.6.17 "Secure channel: Digitally encrypt or sign secure channel data (always)" ensures that the secure channel is always either encrypted or signed. If the client is unable to encrypt or sign the secure channel, it will not be able to establish a logon session with the domain controller. Even though this is good for security, the NSA does not recommend this setting because it requires that all domain controllers in all domains support encryption or signing of the secure channel. The transition team wants to err on the side of caution, so they have accepted the NSA's recommendation and both templates disable this setting.

3.6.18 "Secure channel: Digitally encrypt secure channel data (when possible)" allows all secure channel communication coming from the client to be encrypted. However, even if all traffic cannot be encrypted, the client will still be able to authenticate with the domain controller. Midwest Bank has set this value on their Windows 2000 workstations and is now planning to enable it on the domain controllers when they move to Active Directory. The transition team has decided to accept the NSA's recommendation and enable this setting.

3.6.19 "Secure channel: Digitally sign secure channel data (when possible)" allows all secure channel communication coming from the client to be digitally signed. Both templates have enabled this setting, even though it will be automatically enabled if the encrypt (when possible) value above is enabled.

3.6.20 "Secure channel: Require strong (Windows 2000 or later) session key" requires encryption with strong keys. Since this requires all domain controllers in all trusted domains to support strong encryption keys, the NSA recommends this value be disabled. Midwest Bank's NT 4.0 domain controllers would not be able to use strong encryption keys anyway, so they have also disabled this setting.

3.6.21 "Send unencrypted password to connect to third-party SMB servers" is used for non-Microsoft SMB servers that only support password exchanges in clear text, such as very old Samba servers. The NSA does not recommend using this setting, and instead recommends updating the third-party product. The transition team does not use third-party products with this vulnerability, so they have also set the value to Disabled.

3.6.22 "Smart card removal behavior" governs what happens when a user removes their smart card from the reader. Midwest Bank has not yet implemented smart cards in their environment, but the transition team feels it is reasonable to accept the NSA's recommendation of Lock Workstation.

Audit configuration

3.6.23 "Audit the access of global system objects" assigns SACLs to the global list of shared system resources, such as "mutextes, events, semaphores, and

DOS devices." (Haney, p. 40). These objects are audited in conjunction with the "Audit Object Access" level of the system. The NSA recommends enabling this setting, but Midwest Bank has decided that this level of auditing is not necessary in their environment. They have disabled this setting.

3.6.24 "Audit use of backup and restore privilege" enables auditing the usage of Backup and Recovery rights. By default, the auditing of these rights is disabled because they tend to fill the security log with a great deal of information. Backup of servers in the Midwest Bank environment is automated and restores are tightly controlled, so the transition team feels they are overseeing backups and restores through other compensating controls. As a result, they have not followed the NSA's recommendation and have disabled this setting.

3.6.25 "Shut down system immediately if unable to log security audits" causes the computer to display a STOP error if the machine is unable to write events to the security log. This could be because the log is full, or perhaps for another reason. The NSA recommends the use of this value, but their documentation also recognizes the fact that many environments will choose not to enable this setting.

Media access

3.6.26 "Allowed to eject removable NTFS media" is by default only permitted for Administrators. Neither the NSA nor the transition team change this value.

3.6.27 Enabling the "restrict CD-ROM access to locally logged-on user" value does not allow the CD-ROM drive to be shared. The NSA recommends this value, and the transition team can't think of a reason to share out a print server's CD-ROM. They enable the value.

3.6.28 Enabling the "restrict floppy access to locally logged-on user" value does not allow the floppy drive to be shared. Floppy drives are never shared in Midwest Bank's environment, so they accept the NSA's recommendation and enable this value.

Recovery Console configuration

3.6.29 Normally, a user must log on with the local Administrator account to access the Recovery Console. However, enabling the "Recovery Console: Allow automatic administrative logon" value causes the file system to be automatically available at a DOS prompt when the Recovery Console is accessed. Unfortunately, this gives anyone with physical access and a Windows 2000 CD complete and unaudited access to the file system. Anyone who would be authorized to boot a server into the Recovery Console would have access to the local Administrator password, so they concur with the NSA and disable this

setting.

3.6.30 The Recovery Console does not normally allow the SET command, which allows removable media and wildcards to be used. The "Recovery Console: Allow floppy copy and access to all drives and folders" value enables use of the SET command, which "allows setting of console environments such as AllowWildCards, AllowAllPaths, AllowRemovableMedia, and NoCopyPrompt" (Haney, p. 51). The NSA recommends that this value be disabled, but the transition team has decided that this functionality could be so helpful in a troubleshooting situation that they will set the value to Enabled. Anyone who has physical access to the machine should be authorized to perform these type of troubleshooting tasks.

Software code-signing options

3.6.31 "Unsigned driver installation behavior" governs what happens when an administrator tries to install a driver that hasn't been signed by a recognized authority. The default behavior is "warn but allow installation," which means that the OS will warn the administrator but allow the driver to be installed after the administrator confirms the installation. The NSA recommends that this value be enabled, and the transition team has agreed even though a number of drivers they must use are not signed. In the end, they feel it is probably better to receive warnings than allow a fraudulent driver to be installed.

3.6.32 "Unsigned non-driver installation behavior" governs what happens when an administrator tries to install an application that hasn't been signed by a recognized authority. In this case, the default behavior is "silently succeed," which is recommended by the NSA and used in the transition team's template because many applications commonly used in Midwest Bank's environment aren't signed.

Miscellaneous options

3.6.33 By default, only Administrators are allowed to schedule tasks through the Task Scheduler. However, the "allow server operators to schedule tasks (domain controllers only)" gives users in the Server Operators group the right to use Task Scheduler on domain controllers. This setting is irrelevant in this case because the w2kbase template is not for domain controllers, so the transition team will follow the recommendation of the NSA and leave the setting at Not Defined.

3.6.34 By default, the contents of the pagefile are never cleared or re-created. The "clear virtual memory pagefile when system shuts down" setting zeroes out the pagefile whenever the system restarts. It is intended to destroy any passwords or other confidential information that applications might have left in the pagefile. The NSA recommends to enable it, but in the past when Midwest Bank's central IT group has enabled this setting on Windows NT, clearing the

pagefile added several minutes to a server reboot. On servers with higher amounts of memory, it takes even longer for the pagefile to be cleared. Because the transition team doesn't want to lengthen the time a server reboot takes to such a high degree, they have decided to disable this feature in the w2kbase template.

3.6.35 Normally, users are prevented from installing printer drivers. However, the "Prevent users from installing printer drivers" gives administrators the choice of allowing users to install their own printer drivers. The NSA recommends that this setting be enabled, but regular users will never be installing drivers on servers in the Midwest Bank environment. So the transition team has enabled this setting.

3.6.36 "Strengthen default permissions of global system objects (e.g. Symbolic Links)" strengthens the DACLs on the global list of shared system resources previously mentioned. Non-administrators can read, but are no longer allowed to modify shared objects they did not create. Both the NSA and the w2kbase templates enable this feature.

3.7 Additional Registry entries

The NSA template propagates a number of security-related Registry entries that are not represented in the Security Templates GUI. The transition team chose to include many of these, but not all of them. In addition, they included a few extra entries of their own. All additional Registry entries not in the GUI are located in the [Registry Values] section of a security template. Values in the w2kbase template that depart from or add to the NSA template are represented here in bold.

Setting	NSA template	w2kbase template
Audit warning level	Enabled, 90%	**Disabled**
Remove LMHash from SAM	Enabled	Enabled
Protect kernel object attributes	Enabled	**Disabled**
Protect against name release attacks	Enabled	**Disabled**
Protect against Computer Browser spoofing	Enabled	Enabled
Enable dead gateway detect	Disabled	Disabled
Perform router discovery	Disabled	Disabled
Enable ICMP Redirect	Disabled	Disabled
Disable IP source routing	Enabled, Completely	Enabled, Completely
TCP SYN attack protect	Best protection	**Typical protection**
Max number of retired TCP half-open sockets	160	**N/A**
Max number of TCP half-open sockets	200	**N/A**
TCP connection keep-alive time	3000000 (5 minutes)	**N/A**
Disable media autoplay	Enabled	Enabled
Disable automatic administrator logon	Enabled	**N/A**
Disable OS/2 and POSIX subsystems	N/A	**Enabled**

Table 5

Audit/ACL settings

3.7.1 This is a newly-supported Registry entry for Windows 2000 machines with Service Pack 3 or greater installed. Once the audit log reaches a given percent full, a success audit event with ID 523 is written to the security log. The NSA recommends to set this to 90 percent, but since Midwest Bank does not manually clear their logs they don't feel this setting is necessary in their environment. It is also important to point out that the percentage full is based on the maximum size of the log and not the available space, which means that the maximum log size should not be set to an extremely high value. See the section covering Event Log settings for more information.

3.7.2 Even if the LanManager authentication protocol is not used, an LM password "hash" is generated by default every time a user's password is changed. This weak hash can be easily attacked if the local SAM database is captured. Removing the LM Hash will not affect authentication because LM is not being used in Midwest Bank's environment. Both templates include the entry

that removes the LM Hash from the SAM.

3.7.3 Protect kernel object attributes "ensures that the Object Manager can change the attributes of a kernel object in the Object table for the current process if and only if the previous mode of the caller is kernel mode" (Haney 51). The NSA and Microsoft's Common Criteria-based templates enable this value, but even with all of the documentation they have the transition team is unable to figure out exactly what that is enabling. Even though the NSA template enables the value, one thing the transition team cannot permit is enabling or disabling portions of the OS when they don't fully understand the potential ramifications. They chose to leave this setting out of the w2kbase template.

SMB name resolution attacks

3.7.4 The "Protect against name-release attacks" value helps protect a WINS server from a certain type of DoS attack. Since the w2kbase template is not being designed to protect a WINS server, this setting is disabled.

3.7.5 The "Protect against Computer Browser spoofing" value helps keep malicious users from shutting down browsers by exploiting a vulnerability in the Computer Browser protocol. Since it is possible that a print server or other member server might become a browser, this value is included in the w2kbase template.

TCP/IP stack protection

3.7.6 The "Enable dead gateway" feature allows a Windows 2000 machine to switch to a backup gateway if its default gateway is not accessible. Since Midwest Bank does not use the backup gateway feature in Windows 2000, they have included this value that disables dead gateway detection.

3.7.7 The "Perform router discovery" value enables or disables Windows 2000's use of the Internet Router Discovery Protocol (IRDP) to detect and configure default gateways. Since Midwest Bank does not use backup gateways, this feature has been disabled.

3.7.8 Disabling the "Enable ICMP redirect" value routes ICMP by the shortest path. This seems suitable for Midwest Bank's environment, so the w2kbase template includes this value.

3.7.9 Disable IP source routing" helps stop IP routing attacks. The value of 2 completely disables source routing.

3.7.10 The "Protect against SYN attacks" value adjusts the frequency of TCP SYN-ACK retransmissions. The NSA recommends setting this to its highest value, but the transition team is more concerned about the potential for network

degradation and the other affects this setting could have on their network environment. They are less concerned about the likelihood of a DoS attack because their systems are not directly connected to the Internet and have made significant investments in their firewalls. They have decided not to include this value. For the same reasons, the "keep alive" value will also not be included in the w2kbase template. The "Max number of TCP half-open connections" and "max number of retired half-open connections" will not be necessary because they are only used if the "protect against SYN attacks" value has been changed from the default.

Miscellaneous settings

3.7.11 The "disable media autoplay" setting chiefly refers to stopping the autorun.inf file from automatically executing after a CD-ROM has been inserted into the drive. This has been included in the w2kbase template.

3.7.12 The "automatic administrator logon" feature is never used in the Midwest Bank's environment. Leaving a server without logging off is highly forbidden, and administrators that have done so have had their administrative privileges suspended. Even if a rogue administrator enabled this value, it would be of little use because servers are rarely rebooted and normally are left on the logon screen. As a result, the transition team doesn't feel that this setting is necessary, so it will not be included.

3.7.13 Disabling the OS/2 and POSIX subsystems, if they are not being used, has been suggested ever since the days of Windows NT. They still need to be disabled in Windows 2000, but unlike in Windows NT it only takes a single Registry value. This value is included in the w2kbase template, and it comes from the CC_HiSec_W2K_Server security template (Science Applications International Corporation, p. F-29).

Any Registry entry can be added to a template through the following syntax: Registry key abbreviation, Registry value number, and Registry value. The Registry value numbers appear below (Fossen, Group Policy, p. 51).

Registry value type	Value in template
REG_SZ	1
REG_EXPAND_SZ	2
REG_BINARY	3
REG_DWORD	4
REG_DWORD_LITTLE_ENDIAN	5
REG_LINK	6
REG_MULTI_SZ	7
REG_RESOURCE_LIST	8
REG_FULL_RESOURCE_DESCRIPTOR	9

Table 6

The example for removing OS/2 and POSIX support from the w2kbase template is as follows:

machine\system\currentcontrolset\control\sessionmanager\subsystems\Optional=7,"" (Science Applications International Corporation, p. F-29). Normally, OS/2 and POSIX are listed as values under this key. This removes these values, which in turn disables Windows 2000's OS/2 and POSIX subsystem support.

3.8 Event Log\Settings for Event Logs:

w2kbase = “Database Setting” values
NSA template = “Computer Setting” values

Policy	Database Setting	Computer Setting
Maximum application log size	512000 kilobytes	4194240 kilobytes
Maximum security log size	1024000 kilobytes	4194240 kilobytes
Maximum system log size	512000 kilobytes	4194240 kilobytes
Restrict guest access to application log	Enabled	Enabled
Restrict guest access to security log	Enabled	Enabled
Restrict guest access to system log	Enabled	Enabled
Retention method for application log	As needed	Manually
Retention method for security log	As needed	Manually
Retention method for system log	As needed	Manually
Shut down the computer when the security audit log is full	Disabled	Enabled

Figure 14

By default, the system and application logs are configured for only 512KB of space. The transition team changed the default settings to match the event log policy in their environment. They made several changes that loosen the security assigned by the NSA template. The NSA template increases the maximum log sizes to the maximum of almost 4.2 GB, but the transition team doesn’t feel this is necessary or desired. Midwest Bank’s server administrators don’t want logs to grow to an unmanageable size, or especially to the point where they put a server in jeopardy by filling the hard drives. So the transition team assigns a maximum of 500 MB for the application and system logs. The maximum size for the security log file is doubled, to 1 GB. If all else fails and the log exceeds the maximum, the transition team has set the log files to overwrite the oldest entries as needed. The NSA template stipulates that log files be cleared manually so no entries are lost. However, the Information Security group uses Bindview’s bv-control product to collect logs from all servers and store them in a central location. This ensures that logs are constantly monitored, and that is it not necessary to keep all logs locally on the servers. One setting that remains the same between the two templates is the option that disables Guest access to the event logs.

As the log files are set to overwrite, the setting that causes a STOP error when the security log is full is irrelevant. However, even if the log files were set to clear manually, the transition team would not want this setting to be enabled. Print servers, and the great majority of the other servers in Midwest Bank’s environment, would not be set to enable this setting. It’s felt that enabling this feature has the potential to do more harm then good, especially since anyone who knows this feature is enabled could intentionally generate enough security log activity to bring down a server. If a print server goes down, this will keep the users attached to that server from printing. In the future, if this feature needs to be enabled for an extremely limited scope of servers that host security-sensitive applications, it can be enabled on a case-by-case basis. It is also worth

mentioning that the setting in the template for enabling this feature is not with the Event Log settings, but resides under the Audit Event portion of the template. In the w2kbase.inf template, the setting is CrashOnAuditFull = 0. This value is only invoked if the security log is full, and is not the same value as the “Shut down system immediately if unable to log security audits” setting under Security Options. That value causes a STOP error if the computer is unable to log security events for any reason, not just a full security log.

3.9 Restricted Groups

The Restricted Groups feature is used to lock down group membership. When a groups are added to the Restricted Groups section of a security template and the template is applied, the group and all IDs in it are reset according to the template values. Every time the template settings are refreshed, the membership of groups that have been added to Restricted Groups is also reset. If no one is flagged to be a member of the group, any users in the group will be removed. This is useful for protecting security-sensitive groups.

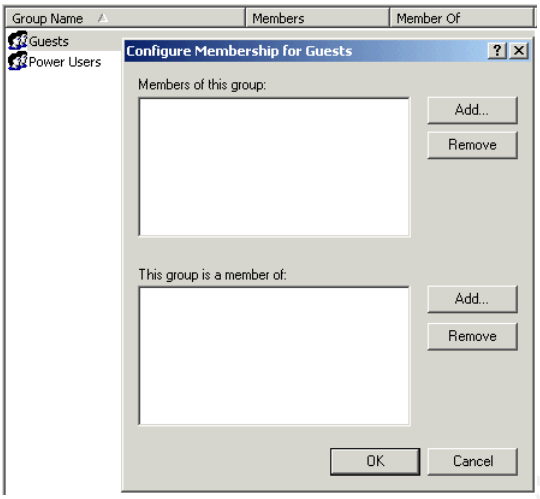

Figure 15

The NSA template places the local Power Users group into Restricted Groups. In addition, the NSA template removes all members of the Power Users group. Every time the template is refreshed, anyone who had previously been added to the Power Users group is automatically removed. The w2kbase template incorporates the NSA's recommendation, but also goes one step farther by placing the Guests group into Restricted Groups and removing all users from it. The syntax for removing all users from the Guests group was copied from Microsoft's CC_HiSec_W2K_Server template (Science Applications International Corporation, p. F-35). It is probably unlikely that a malicious user will attempt to join the Guests group because there are much more tempting targets on the domain, but it doesn't hurt to limit the Guests group because there will never be any legitimate users in it. The section of the w2kbase template also has been changed to use the strings that were mentioned in the User Rights Assignment section. The templates perform the same action, but use different syntax:

Action	NSA template syntax	w2kbase template syntax
Remove all users in Power Users group	*S-1-5-32-547__Memberof =	%SceInfPowerUsers%__Memberof =
Add Power Users to Restricted Groups	*S-1-5-32-547__Members =	%SceInfPowerUsers%__Members =

Table 7

3.10 Registry and file/folder DACLs

The transition team has decided to accept almost all of the NSA's recommendations concerning the discretionary access control lists (DACLs) applied to the Registry and file system. The specific DACL changes included in the w2kbase template are listed in Appendices C and D. The majority of the entries from the NSA template re-establish the default Windows 2000 DACLs from a clean NTFS install. At first this may seem unnecessary, but it is important because the periodic template refresh will be able to reset DACLs that reside in the template. If anyone has made changes to them, those changes can be deleted with a template refresh. This doesn't take the place of vigilant auditing and monitoring, but it is a useful stopgap that ensures unauthorized changes will be overwritten.

The only significant change the NSA makes to file/folder DACLs is the substitution of Authenticated Users for the Users group. By default, Windows 2000 Professional and member servers utilize the Users group when assigning security to regular users. However, Microsoft uses the Authenticated Users group to assign security on domain controllers. The NSA template also makes this substitution in their member server template, and the transition team strongly feels that it is important to carry this forward in their environment.

The majority of the Registry and file/folder DACLs in the w2kbase template are carried over from the NSA's template's DACL recommendations. However, the transition team has customized a few values.

3.10.1 DACLs removed in the w2kbase template

Entries that specifically relate to domain controllers were commented out by putting a semicolon in front of the entry. These changes won't be applied when the w2kbase template is applied. However, the entries are still in the template and could be applied later on a domain controller if so desired. The NSA template assigned a DACL relating to a My Download Files directory, but this directory does not exist on Midwest Bank's servers because they do not have Internet access. In addition, the SNMP-related Registry DACLs in the NSA template were not inserted into the w2kbase template because they refer to vulnerabilities that do not apply to a Windows 2000 installation with Service Pack 2 or greater.

In two instances, Registry DACLs in the NSA template assigned permissions to the Backup Operators local group. Because Midwest Bank does not use Backup Operators, those instances need to have this group removed. It can be done through the Security Templates MMC snap-in, but a faster way is to edit the template manually. Here is one of the values from the NSA template that references the Backup Operators group:

"machine\system\currentcontrolset\control\securepipeservers\winreg",2,"D:PAR(A;CI;KA;;;BA)(A;;KR;;;BO)(A;CI;KA;;;SY)"

The DACL on the above key assigns users or groups the right to remotely access the Registry. If it does not exist, anyone can connect to the Registry. The syntax may look overwhelming at first, but a basic understanding of Security Descriptor Definition Language (SDDL) will prove helpful. A complete discussion of SDDL is outside the scope of this document, but understanding how SDDL is used to assign DACLs can make manipulation of a security template easier. ("Security Descriptor Definition Language: SID Strings.")

For Registry access:

Template abbreviation	Registry key DACL
KA	Key All
KR	Key Read
KW	Key Write
KX	Key Execute

Table 8

For file access:

Template abbreviation	File/folder DACL
FA	File All
FR	File Read
FW	File Write
FX	File Execute

Table 9

For generic DACLs (often used in templates employed by Windows 2000 Setup):

Template abbreviation	Generic DACL
GA	Generic All
GR	Generic Read
GW	Generic Write
GX	Generic Execute

Table 10

(Tables from "Security Descriptor Definition Language: SID Strings.")

The most important information is the abbreviation list of groups:

"AO"	Account operators
"RU"	Alias to grant permissions to accounts using applications compatible with Windows NT 4.0 operating systems
"AN"	Anonymous logon
"AU"	Authenticated users
"BA"	Built-in administrators
"BG"	Built-in guests
"BO"	Backup operators
"BU"	Built-in users
"CA"	Certificate publishers
"CG"	Creator group
"CO"	Creator owner
"DA"	Domain administrators
"DC"	Domain computers
"DD"	Domain controllers
"DG"	Domain guests
"DU"	Domain users
"EA"	Enterprise administrators
"ED"	Enterprise domain controllers
"WD"	Everyone
"PA"	Group Policy administrators
"IU"	Interactively logged-on user
"LA"	Local administrator
"LG"	Local guest
"LS"	Local service account
"SY"	Local system
"NU"	Network logon user
"NO"	Network configuration operators
"NS"	Network service account
"PO"	Printer operators
"PS"	Principal self
"PU"	Power users
"RS"	RAS servers group
"RD"	Terminal server users
"RE"	Replicator
"RC"	Restricted code
"SA"	Schema administrators
"SO"	Server operators
"SU"	Service logon user

Table 11

(Table from “Security Descriptor Definition Language: SID Strings.”)

“BO” is the abbreviation for Backup Operators, so the (A;;KR;;;BO) syntax was removed from the value. The value that went into the w2kbase template became "machine\system\currentcontrolset\control\securepipeservers\winreg",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)". The AsrCommands Registry key from the NSA template also had its reference to Backup Operators removed in this way. Since

the syntax can be complicated, it is recommended to use the Security Templates snap-in to automatically create SDDL syntax from scratch. However, if the syntax that will provide the appropriate access is already known, groups can easily be added and removed from the template by hand. It is wise to check the result in the Security Templates snap-in before propagating the template to a machine.

3.10.2 Added DACLs in the w2kbase template

The remaining changes in the w2kbase security template are new DACLs that were added to customize a server in the Midwest Bank environment. For example, the DACL for the C drive is copied for use on the D and E drives. In Midwest Bank's environment, software is installed in a D:\Program Files folder, unless the software requires installation in another location. On A1PRINT01, the print spooler is moved to E:\spool\print so it will have enough room to grow and not impact the operating system. Because the print spooler is moved to the E drive on Midwest Bank's print servers, the DACL for the default print spooler location is copied to that location.

3.11 Service configuration

The NSA documentation recommends disabling any unnecessary services in the environment, but makes no suggestions which services should be disabled because this varies so widely between organizations. The Windows 2000 transition team also wants to disable services that are not needed, but they want to take a different approach. Disabling services is good, but anyone with administrative rights has the power to start these services again. The Windows 2000 transition team is most interested in using the w2kbase template to "permanently" disable services that have been identified as forbidden in their environment. A good example is the Telnet Server service. It is certainly useful to have an easy way to get to a command prompt, but this service cannot be used because commands pass in clear text. Even though Information Security has forbidden this service to be in use anywhere in the enterprise, it has occasionally been found enabled on test Windows 2000 servers that were built before the unattended install was finalized. After analyzing the services that are generally running on Windows 2000 servers, the transition team has identified the following services as candidates for removal:

Service name	Purpose, and reason for removal
Telnet Server	Allows access to the command prompt on the target machine. Forbidden because commands are passed in clear text.
NetMeeting Remote Desktop	NetMeeting is not used on servers in the Midwest Bank environment.
CilpBook Server	Allows access to remote ClipBooks. This functionality is not in use anywhere in the Midwest Bank environment.
Automatic Updates	Midwest Bank uses SMS for software deployment.
Background Intelligent Transfer Service (BITS)	Midwest Bank uses SMS for software deployment.
Internet Connection Sharing (ICS)	ICS is not used on servers in the Midwest Bank environment.

Table 12

No one is permitted to run these services, and even administrators should not be able to start them. The answer to this problem lies in this SDDL syntax, using the Telnet Server service as an example:

TlntSvr,4,"D:AR(A;;RPWPDTRC;;;BA)"

The number 4 as the startup type disables the service. The SDDL value in parenthesis gives the built-in Administrator account limited rights to manage the service. However, there is no command that gives rights to the built-in LocalSystem account (SY). Because the LocalSystem account's rights to manage the service have been revoked, an Administrator will not be able to manage this service either. One of the best things about using the security

template in this way is that starting that service is not as easy as simply clicking the Start button. However, it is important to point out how to reverse this setting, in case a service disabled in this fashion turns out to be necessary after all. For example, let's say that the transition team used the w2kbase template to permanently disable the ClipBook service, but found out later that it was needed for some reason. Another security template would need to be applied on top of the w2kbase template with the following values:

```
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1

ClipSrv,2,"D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CC
DCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRS
DRCWDWO;;;SO)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSW
RPWPDTLOCRSDRCWDWO;;;WD)"
```

This is the SDDL syntax that originally set up the permissions for the ClipBook service. For these default values, look in the setup security.inf template in C:\Winnt\Security\templates, because this template was used during Windows 2000 Setup to configure security parameters on the machine. If the setting cannot be found in this file, try looking at the defltsv.inf (Default Server) and ocfiless.inf (Optional Components) templates in C:\Winnt\inf. Measures should be put in place to detect and alert if the w2kbase security database has changed at an unexpected time (not through a planned template refresh).

The Windows 2000 transition team has been very conservative about the services that are not permitted in w2kbase.inf. It is likely that they will recommend disabling other services in addition to the ones disabled here. They are still standardizing their environment across the three domains, and don't want to take the chance of disabling a service that might turn out to be necessary. They know it is easy to push out Registry changes through SMS or run VBScripts that disable services. As Windows 2000 is adopted among more server platforms, more testing will be performed to determine other services that can be stopped permanently. The central IT group needs to undergo a Windows 2000 service audit to determine what services are not necessary in their environment.

4.0 Application of security template

The security template (w2kbase.inf) is kept in the $$\Security\Templates folder on the unattended install distribution point server. Because it resides in this location on the distribution point, it is automatically copied to c:\winnt\security\templates during Windows 2000 Setup. This consolidates management of the template in one central location, as well as ensures that the template will always reside in a known location on the new server. The unattended install uses the cmdlines.txt file to apply hotfixes during Windows 2000 installation, as previously mentioned. The transition team had first planned to use cmdlines.txt to also apply the security template, which had the benefit of ensuring that the template gets applied to every new server before it is joined to the domain or before a user even logs onto the machine. However, it turned out that security templates cannot be applied during Windows 2000 Setup because the Windows Explorer shell needs to be running. So the template was instead applied through a command file called template.cmd, which was placed in the $$\Security folder of the unattended install distribution point server. This file is referenced in the GUIRunOnce section of the unattended setup text file, which will cause the template to automatically be installed the first time a user logs onto the machine.

Line wraps—the commands below are on two lines

```
secedit /configure /db c:\winnt\security\database\w2kbase.sdb /cfg
c:\winnt\security\templates\w2kbase.inf /log c:\winnt\security\logs\w2kbase.log
pause
```

The secedit command is the command-line version of the Security Configuration and Analysis MMC snap-in. It is an extremely useful command that performs tasks which SCA cannot do, such as manually refresh Group Policies, apply only selected portions of a security template, remotely analyze or configure a machine, and analyze or configure a computer through a batch file. Listed are the switches that can be used with the secedit command (Fossen, Group Policy, p. 47)

Secedit switches	Actions performed
/analyze /db *filename* /cfg *filename* /log *logpath* /verbose /quiet	Analyzes system security. /db specifies the security database, /cfg specifies the security template, /log specifies the log file, /verbose shows detailed progress information, and /quiet suppresses screen and log output.
/configure /db *filename* /cfg *filename* /overwrite /areas *area1, area2, etc.* /log *log file* /verbose /quiet	Configures system security. /db specifies the security database, /cfg specifies the security template, /overwrite overwrites an existing security database, /areas allows only portions of the template to be applied, /log specifies the log file, /verbose shows detailed progress information, and /quiet suppresses screen and log output.
/refreshpolicy MACHINE_POLICY	Reapplies system security to the GPO.

USER_POLICY, /enforce	MACHINE_POLICY refreshes security settings for the local computer, USER_POLICY refreshes security settings for the logged-on user, and /enforce refreshes settings even if there have been no security changes.
/export /mergedpolicy /db *filename* /cfg *filename* /areas /log *log file* /verbose /quiet	Exports security settings from a security database to a template file. /mergedpolicy merges and exports both domain and local policy settings, /db specifies the security database, /cfg specifies a template to create, /areas allows only portions of the template to be applied, /log specifies the log file, /verbose shows detailed progress information, and /quiet suppresses screen and log output.
/validate *filename*	Validates the syntax of a security template.

Table 13

So the command file above configures security settings by creating a new security database called w2kbase.sdb, using a security template called w2kbase.inf, and logging output in a log file called w2kbase.log. The log file for this operation will be named w2kbase.log and will be stored in the normal place for log files (c:\winnt\security\logs). The system then pauses so the user can verify the expected result. Results of the secedit command:

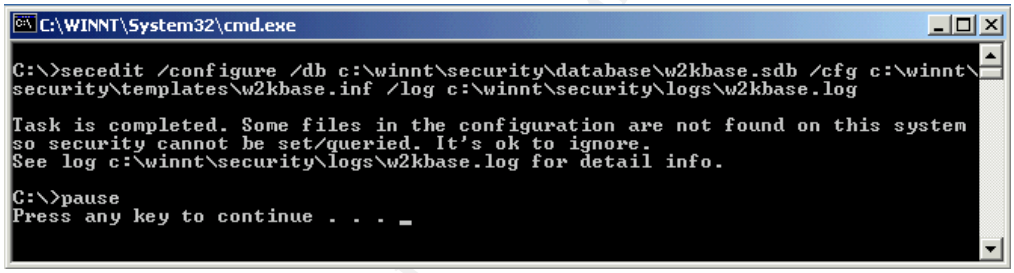

Figure 16

The success message received looks like it could be an error: "Some files in the configuration are not found on this system so security cannot be set/queried. It's OK to ignore." This is an expected result that actually is OK to ignore because not all of the directories and Registry keys referenced in the security template will necessarily exist. In cases where secedit encounters DACL entries that do not exist, it will skip them and continue security configuration on the target machine. To view the operations that secedit performed, open the log file. Here are some examples from the w2kbase.log file that shows the DACLs not found when the above command was performed:

----Configure File Security...
Error setting security on c:\documents and settings\all users\documents\drwatson.
Warning 2: The system cannot find the file specified.
Error setting security on c:\ntbootdd.sys.

Warning 2: The system cannot find the file specified.
Error setting security on c:\program files\resource kit.
Warning 2: The system cannot find the file specified.
Error setting security on c:\winnt\$ntservicepackuninstall$.
Warning 2: The system cannot find the file specified.
Error setting security on c:\winnt\csc.

4.1 Future maintenance/refreshing of w2kbase.inf in the Midwest Bank environment

When a security template is applied to a Windows 2000 server in the Midwest Bank environment, settings are placed in the Local Group Policy Object (GPO). Even though Active Directory is not yet in use, by default the Local Group Policy is automatically reapplied every 90 minutes, with a randomizing factor of up to 30 additional minutes. However, since this is local to the machine and not controlled centrally, the transition team plans to use SMS to make sure the local GPOs are always accurate and that the w2kbase security template is always the latest version. SMS will be used to push out a new version of w2kbase whenever it has been updated. In addition, during the weekly server maintenance period, the secedit command above will be run again on the server. This time, the secedit command will have the /overwrite and /quiet switches so the default.sdb security database will be entirely overwritten. This will help ensure that all servers configured with the w2kbase template have the appropriate values stored in their local GPOs. Whenever the template is updated, the new version of the template will be placed in the $$\Security\Template folder on the unattended install distribution point, so any newly built servers will immediately receive the new security settings.

5. Security template testing

A member server named A1PRINT01 was built with the unattended install. It was configured with the standard print server hardware and software mentioned previously. Because the transition team wants the A1PRINT01 print server to be separate from the production environment during the testing process, the server is racked in Midwest Bank's test lab. This will also keep the existing Windows NT 4.0 print servers on the production environment separated. A1PRINT01 is currently the only print server of any kind in the lab. The lab is isolated from the production network, but network connections to the production environment can be enabled in special circumstances. The lab has a domain controller for all three domains, which were originally installed in this manner:

- Connection to production was activated for the three target domain controllers
- NT 4.0 was installed as a BDC for each domain
- BDCs were synchronized with their domains
- The production network connections were disabled
- The BDCs were promoted to PDCs in the lab

The lab switch is a Cisco Catalyst 5550, with three 24-port blades. An eight-port VLAN was created on the switch for the domain controllers, a workstation with Midwest Bank's standard Windows 2000 image, A1PRINT01, the HP LaserJet 8100's JetDirect LAN card, and the Windows NT 4.0 DHCP/DNS/WINS server. A1PRINT01 was configured in DNS and WINS. A configuration page was printed out for the printer's JetDirect, so it could be configured in WINS/DHCP. The servers have static IP addresses, and the DHCP server assigns IP addresses to the workstation and the printer.

5.1 Security template application test #1: Changes to logon prompts

A member of the transition team logged on with the local Administrator account, applied the w2kbase template, and rebooted the system. When the system is rebooted, it's easy to confirm that changes have made to the logon process. For example, the configured logon banner now appears:

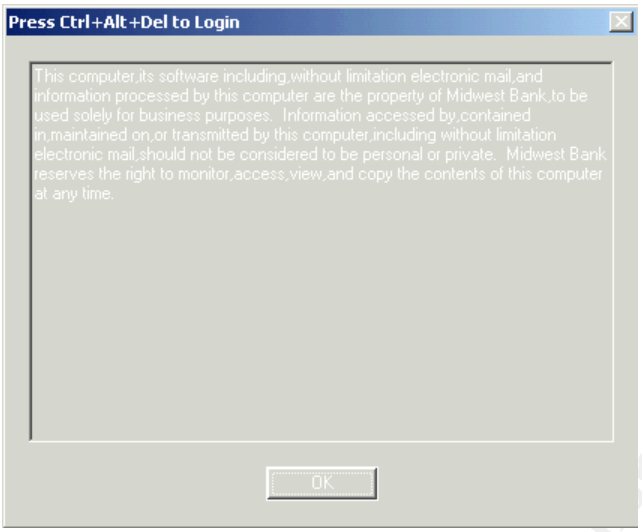

Figure 17

The logon box no longer has the last logged-on user ID. In addition, using the administrator ID is no longer accepted even though the correct password is being used, because the template renamed that account to a1hjs77:

Figure 18

The logon failure message has been moved from to the bottom of the screen, so it can be verified that the administrator ID was used for the logon attempt.

5.2 Security template application test #2: Verifying disabled services

Before applying the security template, the Telnet service was set to the default of Manual. It could be stopped and started successfully by an administrator, as shown below.

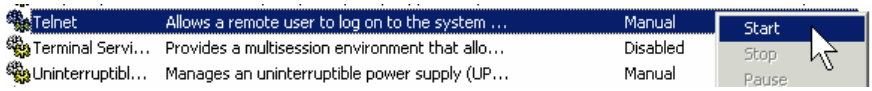

Figure 19

Results in…

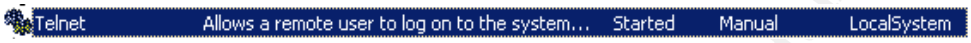

Figure 20

After the security template has been applied, the Telnet service (and the other services referenced in the w2kbase template) are listed in the Services applet without any properties at all. Right-clicking them does not give the choice to start or stop the services. This view has been sorted so the six configured services are shown at the top:

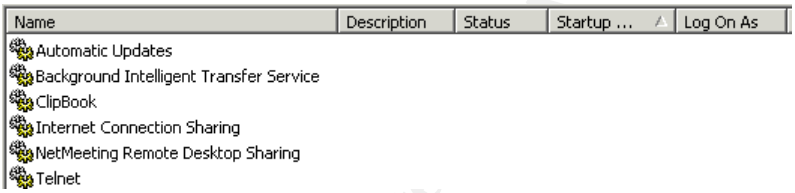

Figure 21

Even though no information is shown in the GUI for these services, it is easy to confirm that they aren't running because they do not appear in Task Manager. No information is displayed for these services because the template revoked the LocalSystem account's rights to stop, start, pause, or even view the properties of these services. The result is that an administrator is also unable to configure the service. Note what happens when the local Administrator simply attempts to view the Telnet service's properties:

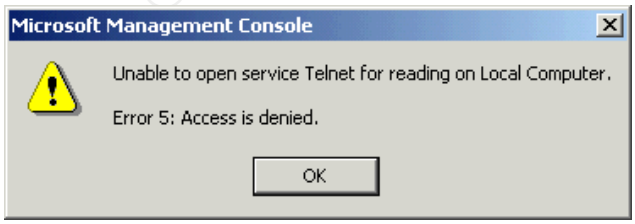

Figure 22

5.3 Security template application test #3: verification of DACL changes

Before the template was applied, NTFS file/folder DACLs were left at the default. For example, shown here are the well-known default NTFS permissions for the root of the C drive in Windows 2000:

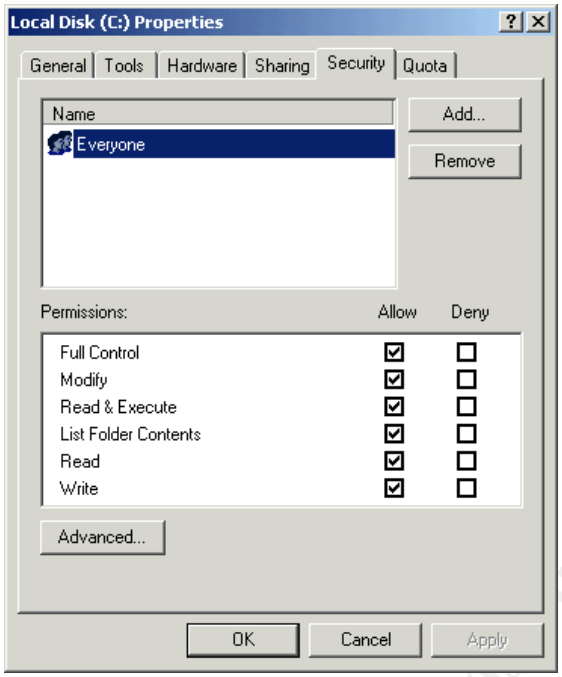

Figure 23

Since the days of Windows NT, the default DACL for the root of the C drive has been Everyone Full Control. Windows 2000 makes a lot of DACL changes that tighten permissions for regular users, but Everyone Full Control remains the default for the root of C. Because there are instances where the root of the C drive can be in the search path, even Microsoft does not recommend keeping the default DACL in this location: “This situation gives rise to a scenario that could enable an attacker to mount a Trojan Horse attack against other users of the same system, but creating a program in the system root with the same name as some commonly used program.” (Microsoft Security Bulletin MS02-064). Even though administrators are the only users that log onto servers in the Midwest Bank environment, there is no reason to leave the default permissions for the root of C. After the template was applied, the new DACL for the root of C is as shown on the next page:

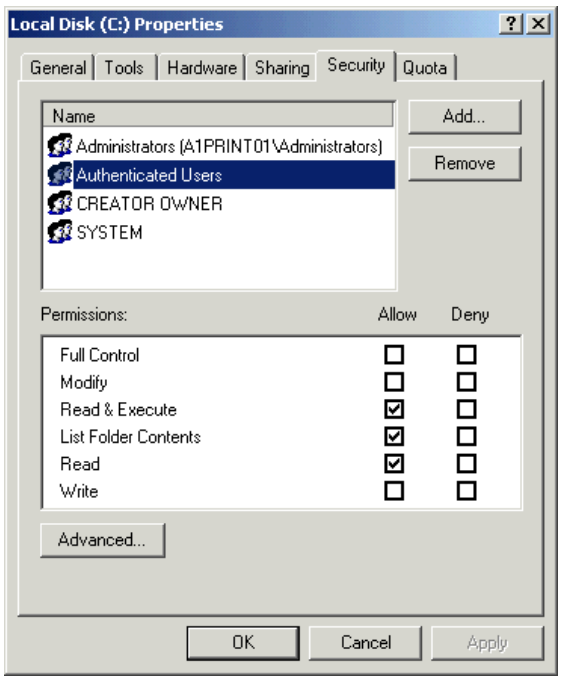

Figure 24

The Everyone group has been completely removed. The Authenticated Users group has been added, as well as the other groups that are necessary when Everyone is no longer being used. Except for the more stringent changes made to C:\Winnt and below in the file system, the DACL entries above propagate throughout the C, D, and E drives.

6. A1PRINT01 functionality testing after successful application of w2kbase.inf

6.1 A1PRINT01 functionality test #1—configuration of a printer on A1PRINT01

The steps used to create the printer on A1PRINT01 are as follows. Screen captures for clicking Next or Continue are not included.

1. A tester with administrative rights opened Printers in Control Panel and clicked Add Printer.
2. The tester clicked Next at the start of the Add Printer wizard.
3. The tester chose Local Printer.
4. The tester chose Create a new Port (Standard TCP/IP Port).

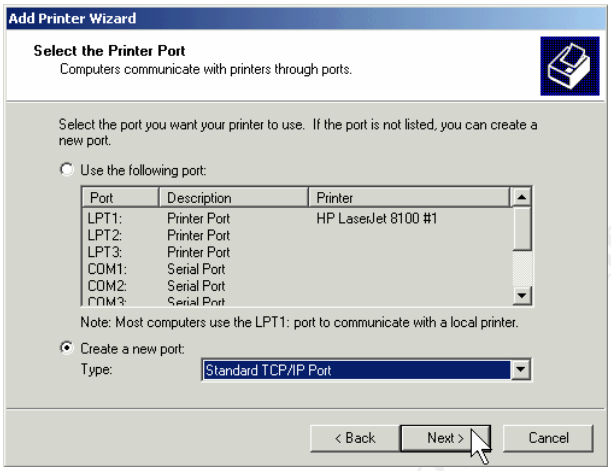

Figure 25

5. The tester clicked Next at the start of the Add Standard TCP/IP Port wizard
6. The JetDirect card's IP address is assigned by DHCP. Its name is J3113A, so the port name is J3113A.midwestbank.org.

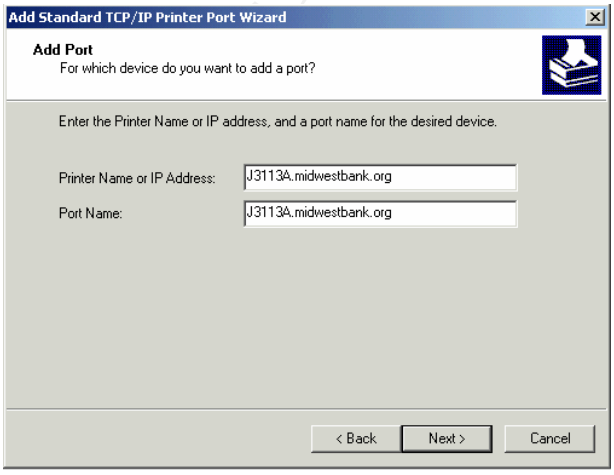

Figure 26

7. The tester selected the printer driver (HP LaserJet 8100 Series PCL).

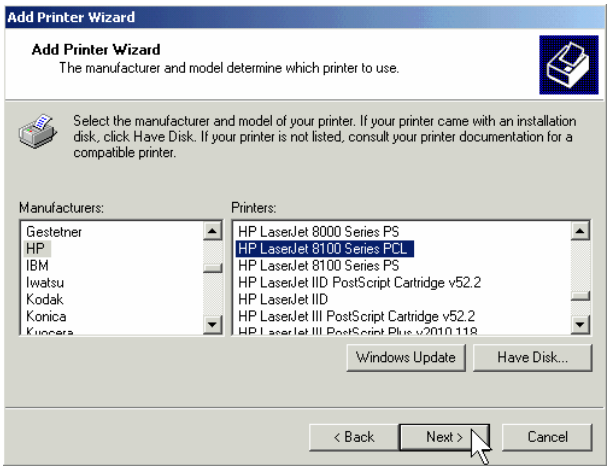

Figure 27

8. The tester named the printer “HP LaserJet 8100 #1.”

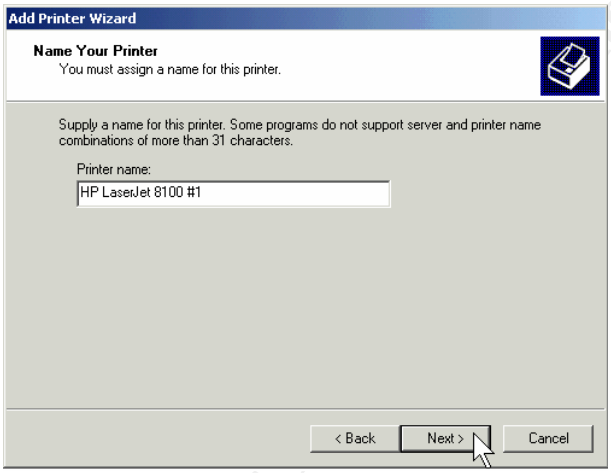

Figure 28

9. The tester shared the printer with the same name (continued on the next page).

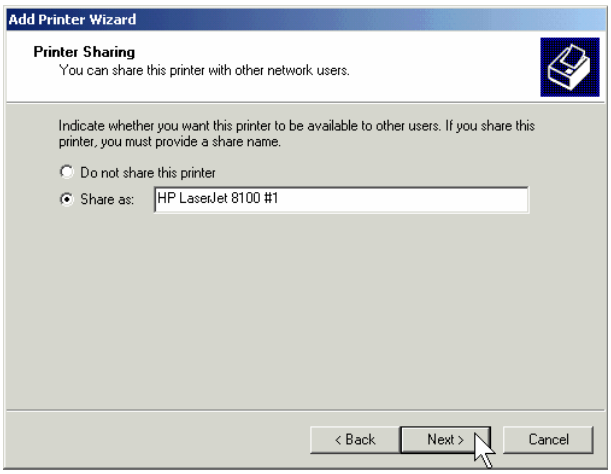

Figure 29

10. OK was clicked at the warning box (share name is too long for MS-DOS workstations).

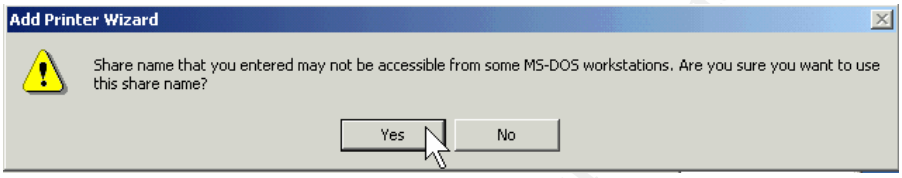

Figure 30

11. A typical location was defined for the printer. Midwest Bank uses the "location" field to input the E911 location of the cubicle the printer inhabits. The "comments" field is the user-friendly location (in this case, on the 3rd floor in the NE quad). Users see the Comments field when they map a printer.

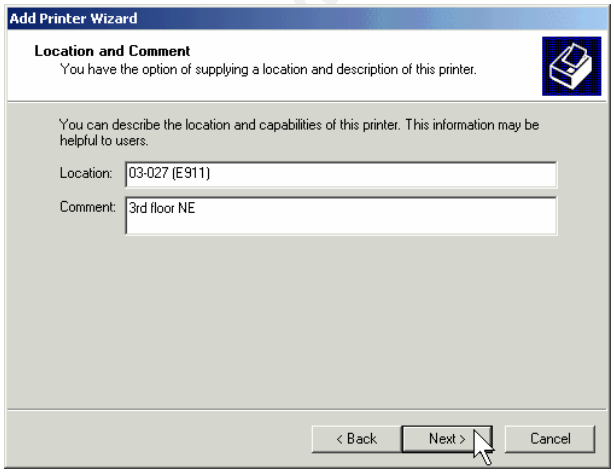

Figure 31

12. The printer was successfully created on A1PRINT01. One printer is now reported in A1PRINT01's Printers folder.

Figure 32

6.2 A1PRINT01 functionality test #2—printer capture by regular user

The users logging on were granted the right to add printer drivers through the workstation's security template.

1. A regular user logged on with the Midwest Bank ID of a1saz00. They opened the Printers folder in Control Panel and clicked on Add Printer.

2. Network Printer was selected.

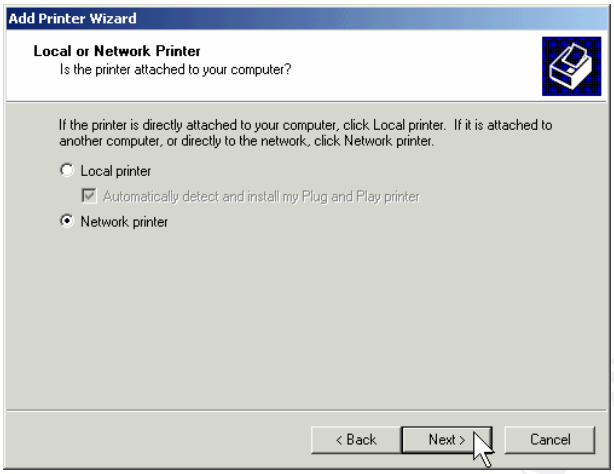

Figure 33

3. The user clicked Next, to browse for the new printer.

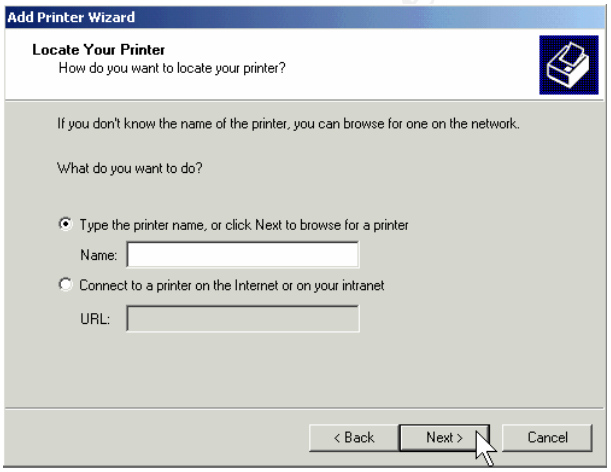

Figure 34

4. The user selected the new printer and clicked OK.

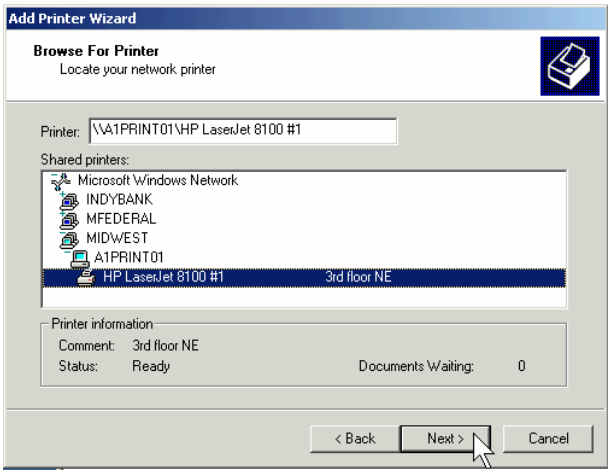

Figure 35

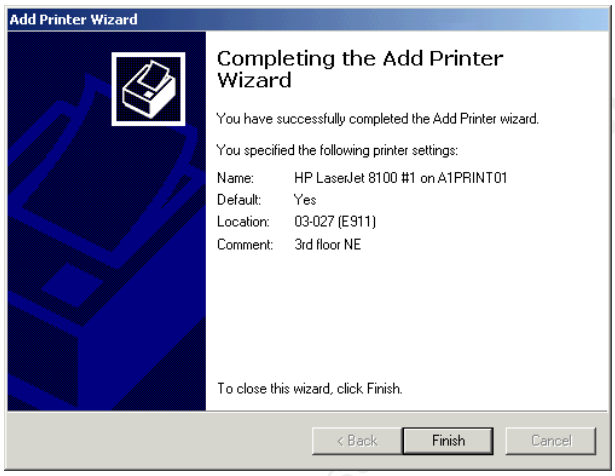

Figure 36

5. Printer capture for a user in the same domain was successful.

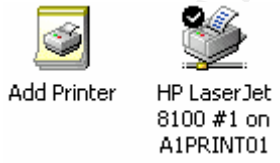

Figure 37

6. Next, a tester logged on with the test account of ibtest from the INDYBANK domain. They followed the steps above to capture the printer on A1PRINT01. The domains showed up in the list, with A1PRINT01 listed under MIDWEST.

However, no printer was listed under A1PRINT01. When A1PRINT01 was double-clicked to browse for the printer, nothing happened.

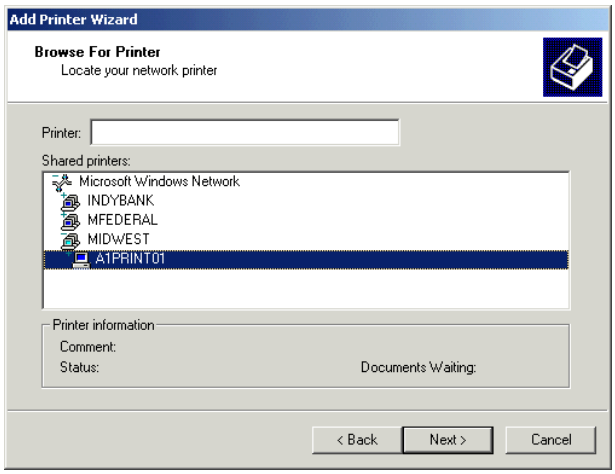

Figure 38

7. When the printer name was typed explicitly into the Printer location prompt at the top of the box, access was denied.

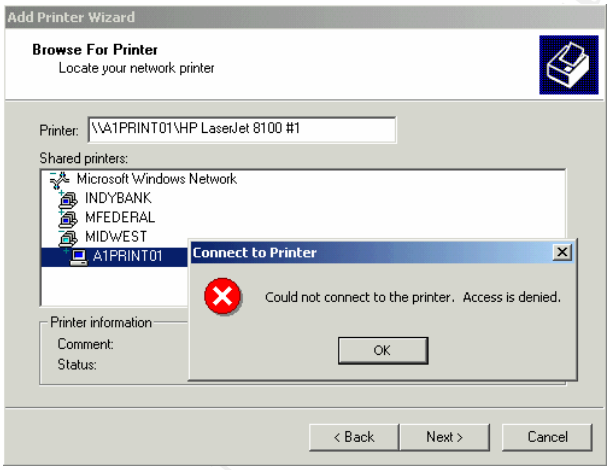

Figure 39

The ibtest user logged off and another test user with administrative rights in the INDYBANK domain logged on. The domain administrator was denied access with the same error.

8. The basic version of Microsoft's Network Monitor is part of the Windows 2000 unattended install. An administrator started a network capture on A1PRINT01 while the tester tried to capture the printer with the ibtest\INDYBANK account. The capture returned the following trace:

```
NBT       NS: Query req. for INDYBANK       <1C>
Netlogon  SAM LOGON request from client
MSRPC     c/o RPC Response:     call 0x1D  context 0x0  hint 0x20  cancels 0x0
SMB       R session setup & X - NT error, System, Error, Code = (396) STATUS_TRUSTED_DOMAIN_FAILURE
```

Capture 1

9. The transition team was very surprised to see a trust relationship issue show up in the capture. Receiving a trust relationship failure message was very puzzling, especially since there never have been any trust relationship issues in the lab. An administrator tested the trust relationships with Domain Monitor, an NT 4.0 Resource Kit utility that analyzes NT-style trust relationships.

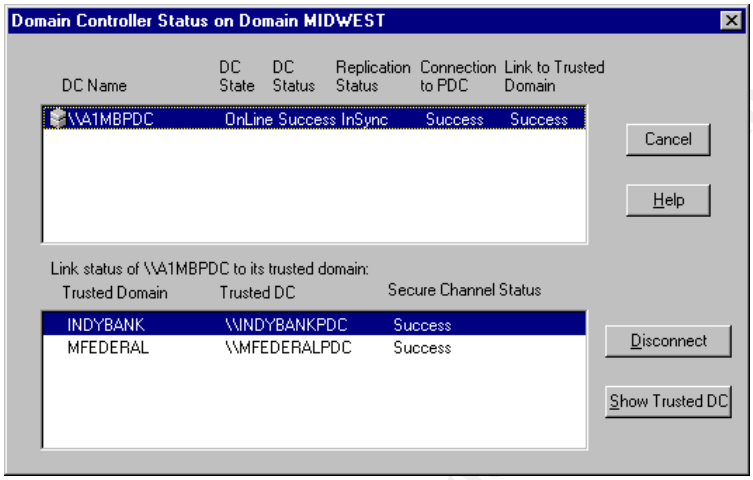

Figure 40

The trust relationship between the three domains appeared to be working properly.

10. To test the trust relationship in a different way, a user logged on as an INDYBANK domain administrator attempted to map to the C$ administrative share on A1PRINT01. This was the result:

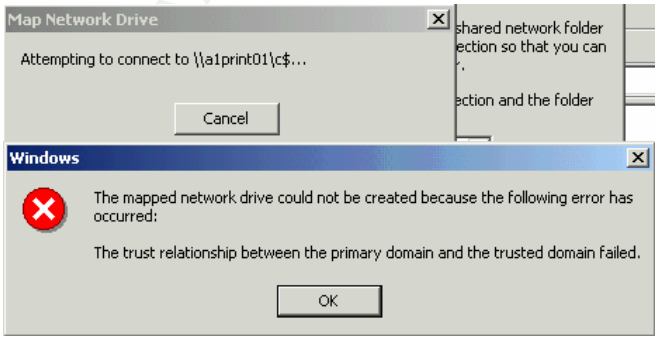

Figure 41

11. Members of the transition team began searching Microsoft's Knowledge Base and Google Groups, but couldn't find anything other than standard trust relationship issues. The team began looking at the new security enhancements to the template. The only enhancement to the security template that specifically had to do with authentication was NTLMv2, so they centered on NTLMv2-related issues. The answer came from Microsoft Knowledge Base article #281480, named "Workstation Does Not Connect to Network Resources Using NTLMv2." According to the article, if NTLM v2 is being used with cross-domain authentication, errors could occur that make the secure channel appear to be broken. Since this is an NT-related issue, a fix was released for the NT domain controllers, but it was not only available through Microsoft Product Support Services and not for download. The transition team changed the w2kbase security template to downgrade the authentication protocol to NTLMv1 and tried capturing the printer again. The capture worked between all domains, as this example of a successful network printer capture shows:

```
R_WINSPOOL   RPC Client call winspool:RpcGetPrinter(..)
R_WINSPOOL   RPC Server response winspool:RpcGetPrinter(..)
R_WINSPOOL   RPC Client call winspool:RpcGetPrinter(..)
NBT          SS: Session Message Cont., 108 Bytes
TCP          .A...., len:    0, seq:3016716758-3016716758,...
R_WINSPOOL   RPC Server response winspool:RpcGetPrinter(..)
SMB          C read & X, FID = 0xd, Read 0x1b4 at 0x00000000
SMB          R read & X, Read 0x1b4
R_WINSPOOL   RPC Client call winspool:RpcClosePrinter(..)
R_WINSPOOL   RPC Server response winspool:RpcClosePrinter(..)
SMB          C close file, FID = 0xd
```

Capture 2

The transition team decided that it is not a prudent course of action to install an unreleased patch on all NT 4.0 domain controllers, in the hopes that NTLMv2 will begin working properly. They decided that the course of action with the least amount of risk is just to downgrade the template to NTLMv1 authentication.

6.3 A1PRINT01 functionality test #1—user printing to the new printer

Since cross-domain authentication had been a problem, the transition team tested first with the ibtest\INDYBANK account. The print queue on HP LaserJet 8100 #1 was paused and a user printed a file to the new printer, which was sent successfully. Pausing the print queue allowed the transition team to verify the sent job in the queue.

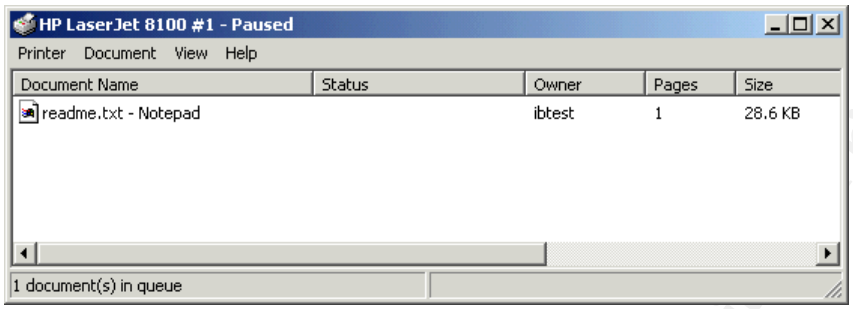

Figure 42

Once the print queue was released, the file printed successfully. Testing with other regular users in the other domains were also successful. The modified template has passed all of the functionality tests.

7. Evaluation of w2kbase.inf

The transition team felt that the NSA template was an excellent template to customize for their environment. The decisions made in the NSA's template greatly enhance security over a default Windows 2000 installation, but the changes made are not so radical that the template is no longer usable for general Windows 2000 servers. After testing the w2kbase security template, the transition team has decided that all of their objectives have been met. Security configuration is consistent, much quicker, and full functionality has been obtained with the Windows 2000 print server. Even though they had to make some compromises, everyone can agree that a Windows 2000 machine with the w2kbase security template is set to a much higher standard than any of the current Windows NT 4.0 servers in production. However, the transition team will be constantly evaluating the template to discover enhancements and make sure no changes have to be developed for the other servers that will receive the template.

The first action item that the transition team suggested is for a comprehensive review of all running services on servers in the Midwest Bank environment. This includes the services currently running in the INDYBANK and MFEDERAL domains. This information is needed to determine what settings can be disabled. In building servers at Midwest Bank, the central IT group was not using a standard to determine what services could be disabled. They were just making a judgement call and disabling services on a need-by-need basis. The Windows 2000 transition team recommended that a standard be put into place. Depending on what information is retrieved, if it is determined that a subset of services is never needed in the environment, they can be disabled through the Service configuration part of the template. If a service is needed in some places but not in others, VBScripts can be written that stop the service and change the Startup value in the Registry to 4. The transition team already has identified some services which may not be necessary, and these services have been identified in Appendix E.

It is also been suggested by the transition team that the DoS TCP/IP settings will need to be tested in the Midwest Bank environment. This is a lower priority than disabling services, because disabling services will likely free up resources on the print server and improve functionality. The threat being protected against by the TCP/IP settings is more remote, and may have a cost in increased network utilization and decreased throughput. However, an internal DoS attack is such an easy attack to launch that it is necessary to address this issue.

When Active Directory is online, the security template being used today at Midwest Bank will greatly change. Since Midwest Bank will be a heterogeneous Windows 2000 environment, they will be able to tighten security much further. In addition, they will have the choice of using domain GPOs in lieu of security templates. Active Directory domain-based GPOs are designed for remote

administration, so the pushing and reapplication of the w2kbase security template will likely no longer be needed. But it is possible for security templates to still play a significant role on servers in an Active Directory domain. Once the security template is changed to remove the NT-compatible values, portions of it could be imported into the Default Domain GPO or other domain-level GPOs. This would save time in creating group policies, and it would already contain many, if not all, of the necessary security configuration values. Security templates can also be used to optimize group policy propagation. Since domain GPOs are propagated and applied every time a machine boots, it may be preferable to take a core group of security parameters that are not expected to change and package them in a security template that is still applied after an unattended install. Instead of using domain-level GPOs, these policies would be propagated when the machine boots through the local GPO. This would result in less domain-level GPO propagation, which could save network bandwidth and save time when a user is logging onto the machine. If it is necessary to change settings that were deployed by the security template, the security template could either be pushed again or domain-level GPOs could be used to override it. This will save time when a user logs onto the machine, save network bandwidth, and cause less GPOs to have to be applied to the machine.

Works Cited:

Fossen, Jason. Securing Windows: Windows 2000/XP Active Directory. SANS Institute. August 2002: 21-29, 92-93.

Fossen, Jason. Securing Windows: Windows 2000/XP Group Policy and DNS. SANS Institute. August 2002: 35-53, 99-111.

Haney, J. "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set." National Security Administration. Version 1.2. 3 December 2002. URL: http://www.nsa.gov/snac/win2k/guides/w2k-3.pdf.

Microsoft Developers Network (MSDN). "Security Descriptor Definition Language: ACE Strings." February 2003. URL: http://msdn.microsoft.com/library/en-us/security/security/ace_strings.asp.

Microsoft Developers Network (MSDN). "Security Descriptor Definition Language: SID Strings." February 2003. URL: http://msdn.microsoft.com/library/en-us/security/security/sid_strings.asp.

National Security Administration. W2K Server.inf security template. 5 March 2003. URL: http://www.nsa.gov/snac/win2k/guides/inf/w2k_server.inf.

Science Applications International Corporation. "Windows 2000 Common Criteria Secure Configuration Guide." Version 1.0. 4 October 2002. URL: http://download.microsoft.com/download/8/c/c/8cc94365-13d6-4975-bf69-9d4cd16a01a7/W2kCCSCG.pdf.

"Windows 2000 Default Permissions Could Allow Trojan Horse Program (Q327522)." Microsoft Security Bulletin MS02-064. Version 1.0. 30 October 2002. URL: http://www.microsoft.com/technet/security/bulletin/MS02-064.asp.

"Workstation Does Not Connect to Shared Resources Using NTLMv2." Microsoft Knowledge Base Article #281480. 16 October 2002. URL: http://support.microsoft.com/default.aspx?scid=kb;[LN];281480.

Appendix A

Original W2K Server.inf security template, provided by the NSA:

```
; (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
;
;  Nov. 2002 -
;       In the Registry section, corrected the
;       MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Perflib to give
;       Creator Owner Full Control on Subkeys only.

; 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 =
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-1-5-32-545,*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 =
[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;OI
CI;0x1200a9;;;BU)"
"%SystemRoot%\$NtServicePackUninstall$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;F
A;;;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;;;S
Y)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)
(A;OICI;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;F
A;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\Registration",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OIC
I;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;F
A;;;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;OI
CI;0x1200a9;;;BU)"
"%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;GXG
R;;;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;0x
1200a9;;;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;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;OICI;0x1200a9;;;BU)"
"%SystemDrive%\IO.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\MSDOS.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;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;;CCDCWP;;;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;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson\drwtsn32.log",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(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;CCDCLCSWR
PSDRC;;;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;;;BU)"
"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;CII
O;KA;;;CO)"
"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;;;BU)"
"machine\system\clone",1,"D:AR"
"machine\system\controlset001",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;K
A;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset002",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;K
A;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset003",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;K
A;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset004",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;K
A;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset005",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;K
A;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset006",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;K
A;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset007",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;K
A;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset008",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;K
A;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset009",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;K
A;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset010",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;K
A;;;SY)(A;CI;KR;;;BU)"
"machine\system\currentcontrolset\control\securepipeservers\winreg",2,"D:PAR(
A;CI;KA;;;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)"
[Registry Values]
MACHINE\System\CurrentControlSet\Control\Session Manager\EnhancedSecurityLevel=4,1
MACHINE\System\CurrentControlSet\Services\Eventlog\Security\WarningLevel=4,90
MACHINE\System\CurrentControlSet\Services\MrxSmb\Parameters\RefuseReset=4,1
MACHINE\System\CurrentControlSet\Services\NetBT\Parameters\NoNameReleaseOnDemand=4,1
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=4,2
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=4,300000
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=4,2
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen=4,200
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetired=4,160
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\Enabl
eForcedLogOff=4,1

Appendix B

The w2kbase.inf security template (production version)

```
; w2kbase.inf
; Midwest Bank W2K security template.  Included in unattended installation
; procedure.  Meant for application to member Windows 2000 Advanced Servers,
; joined to a Windows NT 4.0 domain.
;
; Version 1.1; revised 4/3/03
; created by the Windows 2000 transition team
;
; Revision history:
;
; version 1.0 - template was created for W2K print servers, to serve as base
; security for other Windows 2000 Advanced Servers.  Based on W2K Server.inf
; template provided by the NSA, then enhanced with customizations for our
; environment. Documented every entry in the template.  Created revision history.
;
; version 1.1 - found that enabling NTLMv2 causes problems with mapping some
; shares in a cross-domain Windows NT 4.0 environment.  Problem is
; documented in Microsoft KB article #281480.  Rolling authentication
; protocol back to NTLMv1.

[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[Profile Description]
Description=Security template for Midwest Bank Windows 2000 member servers,
without Active Directory

[System Access]
MinimumPasswordAge = 0
MaximumPasswordAge = 31
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 10
LockoutBadCount = 3
ResetLockoutCount = 99999
LockoutDuration = -1
RequireLogonToChangePassword = 0
NewAdministratorName = "a1hjs77"
NewGuestName = "Adminstrator"
ClearTextPassword = 0
```

```
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 2
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 0
AuditDSAccess = 0
AuditAccountLogon = 3
CrashOnAuditFull = 0

[Strings]
SceInfAdministrator = Administrator
SceInfAdmins = Administrators
SceInfAcountOp = Account Operators
SceInfAuthUsers = Authenticated Users
SceInfBackupOp = Backup Operators
SceInfDomainAdmins = Domain Admins
SceInfDomainGuests = Domain Guests
SceInfDomainUsers = Domain Users
SceInfEveryone = Everyone
SceInfGuests = Guests
SceInfGuest = Guest
SceInfPowerUsers = Power Users
SceInfPrintOp = Print Operators
SceInfReplicator = Replicator
SceInfServerOp = Server Operators
SceInfUsers = Users

[Privilege Rights]
seassignprimarytokenprivilege =
seauditprivilege =
sebackupprivilege = %SceInfAdmins%
sebatchlogonright =
sechangenotifyprivilege = %SceInfUsers%
secreatepagefileprivilege = %SceInfAdmins%
secreatepermanentprivilege =
secreatetokenprivilege =
sedebugprivilege =
sedenybatchlogonright =
sedenyinteractivelogonright =
sedenynetworklogonright =
sedenyservicelogonright =
seenabledelegationprivilege =
```

seincreasebasepriorityprivilege = %SceInfAdmins%
seincreasequotaprivilege = %SceInfAdmins%
seinteractivelogonright = %SceInfAdmins%
seloaddriverprivilege = %SceInfAdmins%
selockmemoryprivilege =
semachineaccountprivilege =
senetworklogonright = %SceInfUsers%,%SceInfAdmins%
seprofilesingleprocessprivilege = %SceInfAdmins%
seremoteshutdownprivilege = %SceInfAdmins%
serestoreprivilege = %SceInfAdmins%
sesecurityprivilege = %SceInfAdmins%
seservicelogonright =
seshutdownprivilege = %SceInfAdmins%
sesyncagentprivilege =
sesystemenvironmentprivilege = %SceInfAdmins%
sesystemprofileprivilege = %SceInfAdmins%
sesystemtimeprivilege = %SceInfAdmins%
setakeownershipprivilege = %SceInfAdmins%
setcbprivilege =
seundockprivilege =

[Registry Values]
machine\software\microsoft\driver signing\policy=3,1
machine\software\microsoft\non-driver signing\policy=3,0
machine\software\microsoft\windows
nt\currentversion\setup\recoveryconsole\securitylevel=4,0
machine\software\microsoft\windows
nt\currentversion\setup\recoveryconsole\setcommand=4,1
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\dontdisplayl
astusername=4,1
machine\software\microsoft\windows\currentversion\policies\system\legalnoticec
aption=1,Press Ctrl+Alt+Del to Login

machine\software\microsoft\windows\currentversion\policies\system\legalnoticetext=1,This computer,its software including,without limitation electronic mail,and information processed by this computer are the property of Midwest Bank, to be used solely for business purposes. Information accessed by,contained in,maintained on,or transmitted by this computer,including without limitation electronic mail,should not be considered to be personal or private. Midwest Bank reserves the right to monitor,access,view,and copy the contents of this computer at any time.
machine\system\currentcontrolset\control\lsa\auditbaseobjects=4,0
machine\system\currentcontrolset\control\lsa\crashonauditfail=4,0
machine\system\currentControlSet\Control\lsa\NoLMHash\bar=4,0
machine\system\currentcontrolset\control\lsa\fullprivilegeauditing=3,0
machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel=4,2
machine\system\currentcontrolset\control\lsa\restrictanonymous=4,1
machine\system\currentcontrolset\control\print\providers\lanman print services\servers\addprinterdrivers=4,0
machine\system\currentcontrolset\control\session manager\memory management\clearpagefileatshutdown=4,0
machine\system\currentcontrolset\control\session manager\protectionmode=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect=4,15
machine\system\currentcontrolset\services\lanmanserver\parameters\enableforcedlogoff=4,1
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\system\currentcontrolset\control\sessionmanager\subsystems\Optional=7,""

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=4,255
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=4,2

[System Log]
MaximumLogSize = 512000
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 1024000
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 512000
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1

[Group Membership]
%SceInfPowerUsers%__Memberof =
%SceInfPowerUsers%__Members =
%SceInfGuests%__Memberof =
%SceInfGuests%__Members =

[Registry Keys]
"CLASSES_ROOT",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\software",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\software\microsoft\netdde",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
"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\protected storage system provider",1,"D:AR"
"machine\software\microsoft\windows\currentversion\installer",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"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 NT\CurrentVersion\AsrCommands",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"

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

[File Security]
"%ProgramFiles%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;
FA;;;CO)(A;OICI;FA;;;SY)"

"D:\Program
Files",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OI
CI;FA;;;SY)"
"%SystemDrive%\Program Files\Resource
Kit",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\secedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;
FA;;;CO)(A;OICI;FA;;;SY)"
"D:\",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OI
CI;FA;;;SY)"
"E:\",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OI
CI;FA;;;SY)"
"%SystemRoot%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;F
A;;;CO)(A;OICI;FA;;;SY)"
"%SystemDirectory%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICII
O;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemDrive%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;CI;DCLCWP;;;AU)(A;OICII
O;FA;;;CO)(A;OICI;FA;;;SY)"
;"%SystemDirectory%\appmgmt",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;A
U)(A;OICI;FA;;;SY)"
"%SystemDirectory%\dllcache",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;
GA;;;CO)"
"%SystemDirectory%\config",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\DTCLog",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU
)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemDirectory%\GroupPolicy",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;
;;AU)(A;OICI;FA;;;SY)"
"%SystemDirectory%\ias",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;
CO)"
"%SystemDirectory%\Ntbackup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\NTMSData",0,"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%\regedt32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\ReinstallBackups",1,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXG
R;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\rsh.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)"
"%SystemDrive%\Inetpub",1,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;
FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\Setup",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(
A;OICI;FA;;;SY)"
;"%SystemDirectory%\repl",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;
OICI;FA;;;SY)"
;"%SystemDirectory%\repl\export",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;
AU)(A;OICI;0x1200a9;;;RE)(A;OICI;FA;;;SY)"

;"%SystemDirectory%\repl\import",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;0x1301bf;;;RE)(A;OICI;FA;;;SY)"
"%SystemDirectory%\spool\Printers",2,"D:PAR(A;OICI;FA;;;BA)(A;CI;DCLCSWWPLO;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"E:\spool\printers",2,"D:PAR(A;OICI;FA;;;BA)(A;CI;DCLCSWWPLO;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemDrive%\boot.ini",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"c:\boot.ini",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\autoexec.bat",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"c:\autoexec.bat",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
"%SystemDrive%\config.sys",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;;CCSWWPLORC;;;AU)(A;;FA;;;SY)"
"%SystemDrive%\IO.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
"%SystemDrive%\MSDOS.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
"%SystemDrive%\System Volume Information",1,"D:PAR"
"%SystemDrive%\Documents and Settings",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\Default User",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(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",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson\drwtsn32.log",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1301bf;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;DCLCWP;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemDrive%\ntdetect.com",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"c:\ntdetect.com",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemDrive%\ntldr",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"c:\ntldr",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"%SystemRoot%\$NtServicePackUninstall$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\$NtUninstallQ323172$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\$NtUninstallQ323255$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\$NtUninstallQ326830$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"

"%SystemRoot%\$NtUninstallQ326886$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\$NtUninstallQ328310$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\$NtUninstallQ329115$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\$NtUninstallQ329170$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\$NtUninstallQ810833$",2,"D:PAR(A;OICI;FA;;;BA)(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;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
;"%SystemRoot%\debug\UserMode",0,"D:PAR(A;OICI;FA;;;BA)(A;;CCDCWP;;;AU)(A;OIIO;DCLC;;;AU)(A;OICI;FA;;;SY)"
;"%SystemRoot%\NTDS",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
;"%SystemRoot%\SYSVOL",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
;"%SystemRoot%\SYSVOL\domain\Policies",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;0x1301bf;;;PA)(A;OICI;FA;;;SY)"
"%SystemRoot%\security",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemRoot%\Tasks",1,"D:AR"
"%SystemRoot%\Offline Web Pages",1,"D:AR(A;OICI;FA;;;WD)"
"%SystemRoot%\regedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;CI;DCLCWP;;;AU)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)"
"%SystemRoot%\repair",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\Registration",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FR;;;AU)(A;OICI;FA;;;SY)"
"c:\ntbootdd.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"

[Service General Setting]
TlntSvr,4,"D:AR(A;;RPWPDTRC;;;BA)"
ClipSrv,4,"D:AR(A;;RPWPDTRC;;;BA)"
mnmsrvc,4,"D:AR(A;;RPWPDTRC;;;BA)"
BITS,4,"D:AR(A;;RPWPDTRC;;;BA)"
wuauserv,4,"D:AR(A;;RPWPDTRC;;;BA)"
SharedAccess,4,"D:AR(A;;RPWPDTRC;;;BA)"

Appendix C: Registry permissions configured by the w2kbase template

Values from the NSA template have been reprinted from the Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set (Haney, p. 76-79). Some values in this table have been moved around for greater readability, so the w2kbase template values have been re-sorted to match.

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
CLASSES_ROOT Alias to MACHINE\SOFTWARE\Classes. Contains file associations and COM (Common Object Model) associations.	Administrators CREATOR OWNER SYSTEM	Full Control Full Control (Subkeys only) Full Control	Replace
\MACHINE\SOFTWARE Contains information about the software installed on the local system.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Replace
\MACHINE\SOFTWARE\Microsoft\Net DDE Settings for Network Dynamic Data Exchange, which is a protocol that allows applications to exchange data.	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SOFTWARE\Microsoft\OS/ 2 Subsystem for NT Contains support for OS/2 standards. Even if this key is removed, it will reappear at next boot up.	Administrators CREATOR OWNER SYSTEM	Full Control Full Control (Subkeys only) Full Control	Replace
\MACHINE\SOFTWARE\Microsoft\ Protected Storage System Provider Used to protect user data. Inaccessible.	Ignore		Ignore
\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer Contains configuration information for the Windows Installer.	Administrators SYSTEM Users	Full Control Full Control Read	Propagate

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
\MACHINE\SYSTEM Stores values for the current control set or control sets that have been previously used to start Windows 2000.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Replace
\MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\AsrCommands Automatic Server Recovery commands. Rights for the Backup Operators built-in group were removed in the w2kbase security template.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Replace
\MACHINE\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\Perflib Parameters for the Performance Library, which collects information for Performance Monitor. Contains a language code subkey for each spoken language configured on the Windows 2000 system. For example, a subkey named 009 contains counters and descriptions for the language code English (United States).	Administrators INTERACTIVE CREATOR OWNER SYSTEM	Full Control Read Full Control (Subkeys only) Full Control	Replace
\MACHINE\SOFTWARE\Microsoft\ Windows\CurrentVersion\Group Policy Contains data for Group Policy settings that configure the Group Policy components of Windows 2000. Contains subkeys representing each of the client-side extensions used to create settings in Group Policy.	Administrators Authenticated Users SYSTEM	Full Control Read Full Control	Propagate
USERS\.DEFAULT Profile that is used while the Windows 2000 CTRL+ALT+DEL logon message is displayed.	Administrators Users CREATOR OWNER SYSTEM	Full Control Read Full Control (Subkeys only) Full Control	Replace

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
USERS\.DEFAULT\Software\Microsoft\ Protected Storage Systems Provider Used to protect user data. Inaccessible.	Ignore		Ignore
\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies Stores registry entries managed by Group Policy. Manages entries for the following subkeys: HKLM\SOFTWARE\Policies HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies HKCU\SOFTWARE\Policies HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	Administrators Authenticated Users SYSTEM	Full Control Read Full Control	Propagate
\MACHINE\SYSTEM\controlset001 Contains a control set that may be used to start and run Windows 2000.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset002 Contains a control set that may be used to start and run Windows 2000.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset003 Contains a control set that may be used to start and run Windows 2000.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset004 Contains a control set that may be used to start and run Windows 2000.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
\MACHINE\SYSTEM\controlset005 Contains a control set that may be used to start and run Windows 2000.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset006 Contains a control set that may be used to start and run Windows 2000.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset007 Contains a control set that may be used to start and run Windows 2000.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset008 Contains a control set that may be used to start and run Windows 2000.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset009 Contains a control set that may be used to start and run Windows 2000.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\controlset010 Contains a control set that may be used to start and run Windows 2000.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
\MACHINE\SYSTEM\clone	Ignore		Ignore

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
\MACHINE\SYSTEM\CurrentControlSet\ Control\SecurePipeServers\winreg The security permissions set on this key define which users or groups can connect to the system for remote registry access. If the key does not exist, anyone can remotely connect to the registry. It is highly recommended that only administrators have remote access to the registry. Rights for the Backup Operators built-in group were removed in the w2kbase security template.	Administrators SYSTEM	Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Control\Wmi\Security Security settings for the Windows Management Instrumentation (WMI). WMI is the Microsoft implementation of Web-Based Enterprise Management (WBEM).	Administrators CREATOR OWNER SYSTEM	Full Control Full Control Full Control	Replace
\MACHINE\SYSTEM\CurrentControlSet\Enum Contains configuration data for hardware devices installed on the system. Changing permissions on this key may result in damage to the Plug and Play function of Windows 2000.	Ignore		Ignore
\MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles Contains system hardware profiles (changes to the initial hardware configuration stored in the Software and System keys).	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Read	Propagate
USERS\.DEFAULT\Software\Microsoft\ NetDDE Settings for Network Dynamic Data Exchange, which is a protocol that allows applications to exchange data.	Administrators SYSTEM	Full Control Full Control	Replace

Table 14

Appendix D: File/folder permissions configured by the w2kbase template

Values from the NSA template have been reprinted from the Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set (Haney, p. 88-94). Some values in this table have been moved around for greater readability, so the w2kbase template values have been re-sorted to match the table. Values that are different from the NSA's template are noted in the table.

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%ProgramFiles% Folder in which applications are installed. By default, this is %SystemDrive%\Program Files	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Replace
D:\Program Files Midwest Bank procedure dictates that all software installs reside in this folder, when possible. The w2kbase template sets this directory with the same DACL as the default Program Files directory.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Replace
%SystemDrive%\Program Files\Resource Kit Folder where the Windows 2000 server Resource Kit is installed by default.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\secedit.exe Security configuration and analysis tool.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive% Drive on which Windows 2000 is installed. Contains important system startup and configuration files.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Propagate
D:\ and E: In the Midwest Bank environment, the D drive is used for software installs. The w2kbase template sets the same DACLs for the D and E drives as the boot drive.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Propagate

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemRoot% Folder in which the Windows 2000 OS is installed. By default, this is called winnt.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Replace
%SystemDirectory% Contains many operating system DLLs, drivers, and executable programs.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Replace
%SystemDrive%\Temp Folder containing temporary files.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Traverse folder, Create files, Create folders (folders and subfolders)	Replace
%SystemDirectory%\appmgmt Contains application management files used for software installation. This setting is commented out in the w2kbase template.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate
%SystemDirectory%\dllcache Contains copies of protected system files. These copies are used by the System File Checker to repair corrupted or modified system files.	Administrators CREATOR OWNER SYSTEM	Full Control Full Control Full Control	Replace
%SystemDirectory%\config Contains registry hive files.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\DTCLog Log file for MS Distributed Transaction Coordinator, which is required for Microsoft Transaction Server.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Propagate

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemDirectory%\GroupPolicy Folder containing local Group Policy Objects.	Administrators Authenticated Users SYSTEM	Full Control Read, Execute Full Control	Propagate
%SystemDirectory%\ias Contains databases for the Internet Authentication Service.	Administrators CREATOR OWNER SYSTEM	Full Control Full Control Full Control	Replace
%SystemDirectory%\Ntbackup.exe File system backup program.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\NTMSData Default location for the Removable Storage database.	Administrators SYSTEM	Full Control Full Control	Propagate
%SystemDirectory%\rcp.exe Remote copy command.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\Regedt32.exe Registry editing tool	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\ReinstallBackups Contains files used for reinstallations.	Ignore		Ignore
%SystemDirectory%\rsh.exe Program used to execute a remote shell.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDirectory%\rexec.exe Program used to execute remote calls.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\Inetpub IIS web server folder. Only exists if IIS 5.0 is installed. Ignored in this document.	Ignore		Ignore
%SystemDirectory%\Setup Contains setup DLLs.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemDirectory%\repl Folder containing scripts and files to be replicated or that have been replicated. This setting is commented out in the w2kbase template.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate
%SystemDirectory%\repl\export Folder containing scripts and files to be replicated to other replication servers. This setting is commented out in the w2kbase template.	Administrators Replicator SYSTEM Users	Full Control Read, Execute Full Control Read, Execute	Propagate
%SystemDirectory%\repl\import Folder containing scripts and files that have been replicated from other replication servers. This setting is commented out in the w2kbase template.	Administrators Replicator SYSTEM Users	Full Control Modify Full Control Read, Execute	Propagate
%SystemDirectory%\spool\Printers OS default printer spool.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Traverse folder, Read attributes, Read extended attributes, Create files, Create folders (folder and subfolders)	Replace
E:\spool\Printers In the Midwest Bank environment, print servers have their printer spool folders moved to the E: drive, which is reserved just for the printer spool.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Traverse folder, Read attributes, Read extended attributes, Create files, Create folders (folder and subfolders)	Replace
%SystemDrive%\boot.ini **c:\boot.ini** Boot menu.	Administrators SYSTEM	Full Control Full Control	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemDrive%\autoexec.bat c:\autoexec.bat Initialization file for DOS applications.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%SystemDrive%\config.sys c:\config.sys Initialization file for DOS applications.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%SystemDrive%\io.sys Initialization file for DOS applications.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%SystemDrive%\msdos.sys Initialization file for DOS applications.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%SystemDrive%\System Volume Information Accessible only by SYSTEM.	Ignore		Ignore
%SystemDrive%\Documents and Settings Folder containing user and default profiles.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate
%SystemDrive%\Documents and Settings\Default User Folder containing default desktop and profile attributes for users logging on for the first time.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Replace
%SystemDrive%\Documents and Settings\Administrator Folder containing the built-in Administrator profile.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\Documents and Settings\All Users Folder containing desktop and profile attributes for all users.	Administrators SYSTEM Users	Full Control Full Control Read, Execute	Propagate

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson\ drwtsn32.log Dr. Watson application error log file.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control Full Control Modify	Replace
%SystemDrive%\Documents and Settings\All Users\Documents\DrWatson Folder containing the Dr. Watson application error log.	Administrators CREATOR OWNER SYSTEM Users Users	Full Control Full Control (subfolders and files) Full Control Traverse folder, Create files, Create folders (subfolders and files) Read, Execute	Replace
%SystemDrive%\ntdetect.com c:\ntdetect.com Hardware detector during Windows 2000 boot.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\ntldr c:\ntldr Windows 2000 operating system loader.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\$NtServicePackUninstall$ Contains older versions of system files necessary to back off a service pack.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\$NtUninstall (all uninstall folders) Contains uninstall files for hotfixes and other applications.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\CSC Contains all offline files requested by any user on the computer. CSC means “client side caching”.	Administrators SYSTEM	Full Control Full Control	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemRoot%\debug Contains various system and Active Directory logs.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Read, Execute	Propagate
%SystemRoot%\debug\UserMode Contains logs for group policy application to users. This setting is commented out in the w2kbase template.	Administrators SYSTEM Users Users	Full Control Full Control Traverse folder, List folder, Create files (folder only) Create files, Create folders (files only)	Propagate
%SystemRoot%\NTDS Active Directory database folder. This setting is commented out in the w2kbase template.	Administrators SYSTEM	Full Control Full Control	Propagate
%SystemRoot%\SYSVOL Default Active Directory location for files that must be shared throughout a domain. This setting is commented out in the w2kbase template.	Administrators Authenticated Users CREATOR OWNER SYSTEM	Full Control Read, Execute Full Control (subfolders and files) Full Control	Propagate
%SystemRoot%\SYSVOL\domain\Policies Contains group policy objects. This setting is commented out in the w2kbase template.	Administrators Authenticated Users CREATOR OWNER Group Policy Creator Owners SYSTEM	Full Control Read, Execute Full Control (subfolders and files) Modify Full Control	Propagate

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemRoot%\security Contains security templates and analysis databases.	Administrators CREATOR OWNER SYSTEM	Full Control Full Control (subfolders and files) Full Control	Replace
%SystemRoot%\Tasks Folder containing jobs scheduled by Task Scheduler.	Ignore		Ignore
%SystemRoot%\Offline Web Pages Folder containing web pages that have been downloaded for off-line viewing.	Ignore		Ignore
%SystemRoot%\regedit.exe Registry editing tool.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\Temp Folder containing temporary files.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders and files) Full Control Traverse folder, Create files, Create folders (folders and subfolders)	Replace
%SystemRoot%\repair Backup files of SAM database and other important registry and system files to be used during a system repair.	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\Registration Folder containing Component Load Balancing (CLB) registration files read by COM+ applications.	Administrators SYSTEM Users	Full Control Full Control Read	Propagate
C:\ntbootdd.sys Copy of the SCSI device driver. Used when using SCSI or Signature syntax in boot.ini.	Administrators SYSTEM	Full Control Full Control	Replace

Table 15

Appendix E: Windows 2000 services running on A1PRINT01 (after application of the w2kbase template)

On A1PRINT01, the services listed start in the context of the LocalSystem account unless noted differently. If no dependencies are listed for a service, assume that service has no dependencies. For all services listed here with a description, these descriptions reside in the Registry under: HKLM\System\CurrentControlSet\Services*name_of_service*\Description and can be accessed from the Windows 2000 Services applet. The vast majority of these descriptions were included in Windows 2000 by Microsoft. In cases where comments are included, they are by the author. For greater readability, alternating services are shaded light grey.

Startup modes

Automatic: the service is automatically initialized when Windows 2000 is started. The service should always be running, unless it has been manually stopped or was not able to start. This corresponds to a REG_WORD Start value of 2 in the Registry.

Manual—the service does not automatically initialize when Windows 2000 is started. However, it can be started at any time, either manually or by a process that has the authority to start it. This corresponds to a REG_WORD Start value of 3 in the Registry.

Disabled: the service cannot start automatically. However, it still can be started manually by an authorized user. This corresponds to a REG_WORD Start value of 4 in the Registry.

Windows 2000 default services

Service name	Alerter
Display name	Alerter
Description	Notifies selected users and computers of administrative alerts.
Default startup mode	Automatic
Depends on	Workstation
Comments	For administrators to be automatically notified of alerts, this service must be running on their administrative workstation. May be OK to disable on servers.

Service name	AppMgmt
Display name	Application Management
Description	Provides software installation services such as Assign, Publish, and Remove.
Default startup mode	Manual (Started)
Comments	Used by Active Directory for software distribution.

Service name	wuauserv
Display name	Automatic Updates
Description	Enables the download and installation of critical Windows updates. If the service is disabled, the operating system can be manually updated at the Windows Update Web site.
Default startup mode	Automatic (but disabled by template)
Comments	This service is only found on a Windows 2000 machine with Service Pack 3 or greater. This has been disabled by the w2kbase security template.

Service name	BITS
Display name	Background Intelligent Transfer Service
Description	Transfers files in the background using idle network bandwidth. If the service is stopped, features such as Windows Update and MSN Explorer will be unable to automatically download programs and other information. If this service is disabled, any services that explicitly depend on it may fail to transfer files if the do not have a fail safe mechanism to transfer files directly through IE in case BITS has been disabled.
Default startup mode	Automatic (but disabled by template)
Depends on	Remote Procedure Call (RPC), System Event Notification, COM+ Event System, and Windows Management Instrumentation Driver Extensions.
Comments	This service is only found on a Windows 2000 machine with Service Pack 3 or greater. This has been disabled by the w2kbase security template.

Service name	ClipSrv
Display name	ClipBook
Description	Supports ClipBook Viewer, which allows pages to be seen by remote ClipBooks.
Default startup mode	Manual (Stopped), but disabled by template.
Depends on	Network DDE and Network DDE DSDM
Comments	This has been disabled by the w2kbase security template.

Service name	EventSystem
Display name	COM+ Event System
Description	Provides automatic distribution of events to subscribing COM components.
Default startup mode	Manual (Started)
Depends on	Remote Procedure Call (RPC)
Dependent services	System Event Notification

Service name	Browser
Display name	Computer Browser
Description	Maintains an up-to-date list of computers on your network and supplies the list to programs that request it.
Default startup mode	Automatic
Depends on	Server and Workstation
Comments	Necessary for Microsoft Networking to function, and extensively used by legacy applications and the Windows NT 4.0 domain model. In an Active Directory domain, DNS provides this function.

Service name	Dhcp
Display name	DHCP Client
Description	Manages network configuration by registering and updating IP addresses and DNS names.
Default startup mode	Automatic
Comments	Necessary to run even if the server has a static address. Even necessary on DHCP servers.

Service name	Dfs
Display name	Distributed File System
Description	Manages logical volumes distributed across a local or wide area network.
Default startup mode	Automatic
Depends on	Server and Workstation
Comments	Can be used without Active Directory, but Dfs is much more flexible and useful when used in conjunction with Active Directory. May be OK to set to Manual.

Service name	TrkWks
Display name	Distributed Link Tracking Client
Description	Sends notifications of files moving between NTFS volumes in a network domain.
Default startup mode	Automatic
Depends on	Remote Procedure Call (RPC)

Service name	TrkSvr
Display name	Distributed Link Tracking Server
Description	Stores information so that files moved between volumes can be tracked for each volume in the domain.
Default startup mode	Manual (Stopped)
Depends on	Remote Procedure Call (RPC)

Service name	MSDTC
Display name	Distributed Transaction Coordinator
Description	Coordinates transactions that are distributed across two or more databases, message queues, file systems, or other transaction protected resource managers.
Default startup mode	Automatic
Depends on	Remote Procedure Call (RPC) and Security Accounts Manager

Service name	Dnscache
Display name	DNS Client
Description	Resolves and caches Domain Name System (DNS) names.
Default startup mode	Automatic

Service name	Eventlog
Display name	Event Log
Description	Logs event messages issued by programs and Windows. Event Log reports contain information that can be useful in diagnosing problems. Reports are viewed in Event Viewer.
Default startup mode	Automatic
Dependent services	File Replication, SNMP Service, and SNMP Trap Service

Service name	Fax
Display name	Fax Service
Description	Helps you send and receive faxes.
Default startup mode	Manual (Stopped)
Depends on	Plug and Play, Print Spooler, Remote Procedure Call (RPC), and Telephony
Comments	Candidate for disabling, certainly on domain controllers.

Service name	Ntfrs
Display name	File Replication
Description	Maintains file synchronization of file directory contents among multiple servers.
Default startup mode	Manual (Stopped)
Depends on	Event Log and Remote Procedure Call (RPC)
Comments	May be possible to disable on member servers. This is the Windows 2000-version of replication, so this service won't be used until the move to Active Directory.

Service name	cisvc
Display name	Indexing Service
Description	(none)
Default startup mode	Manual (Stopped)
Depends on	Remote Procedure Call (RPC)
Comments	May be possible to disable on member servers.

Service name	SharedAccess
Display name	Internet Connection Sharing
Description	Provides network address translation, addressing, and name resolution services for all computers on your home network through a dial-up connection.
Default startup mode	Manual (Stopped), but disabled by template.
Depends on	Remote Access Connection Manager, Telephony, Plug and Play, and Remote Procedure Call (RPC)
Comments	This has been disabled by the w2kbase security template.

Service name	IsmServ
Display name	Intersite Messaging
Description	Allows sending and receiving messages between Windows Advanced Server sites.
Default startup mode	Disabled
Depends on	Security Accounts Manager

Service name	PolicyAgent
Display name	IPSEC Policy Agent
Description	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.
Default startup mode	Automatic
Depends on	Remote Procedure Call (RPC)
Comments	This service must be running for IPSec to function.

Service name	kdc
Display name	Kerberos Key Distribution Center
Description	Generates session keys and grants service tickets for mutual client/server authentication.
Default startup mode	Disabled
Depends on	Remote Procedure Call (RPC)
Comments	Normally only in use on a domain controller.

Service name	LicenseService
Display name	License Logging Service
Description	(none)
Default startup mode	Automatic

Service name	dmserver
Display name	Logical Disk Manager
Description	Logical Disk Manager Watchdog Service
Default startup mode	Disabled

Service name	Messenger
Display name	Messenger
Description	Sends and receives messages transmitted by administrators or by the Alerter service.
Default startup mode	Automatic
Depends on	Remote Procedure Call (RPC) and Workstation
Comments	For automatic notification of alerts, this service must be running.

Service name	Netlogon
Display name	Net Logon
Description	Supports pass-through authentication of account logon events for computers in a domain.
Default startup mode	Automatic
Depends on	Workstation
Comments	Necessary for logon to the domain

Service name	mnmsrvc
Display name	NetMeeting Remote Desktop Sharing
Description	Allows authorized people to remotely access your Windows desktop using NetMeeting.
Default startup mode	Manual (Stopped), but disabled by template
Comments	This has been disabled by the w2kbase security template.

Service name	Netman
Display name	Network Connections
Description	Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.
Default startup mode	Manual (Started)
Depends on	Remote Procedure Call (RPC)

Service name	NetDDE
Display name	Network DDE
Description	Provides network transport and security for dynamic data exchange (DDE).
Default startup mode	Manual (Stopped)

Depends on	Network DDE DSDM
Dependent services	ClipBook
Comments	Some legacy applications use DDE to transfer information. May be OK to disable if found to be unnecessary in Midwest Bank's environment.

Service name	NetDDEdsdm
Display name	Network DDE DSDM
Description	Manages shared dynamic data exchange and is used by Network DDE
Default startup mode	Manual (Stopped)
Dependent services	Network DDE and ClipBook
Comments	May be OK to disable if found to be unnecessary in Midwest Bank's environment.

Service name	NMSSvc
Display name	NMS Service
Description	(none)
Default startup mode	Automatic
Depends on	Remote Procedure Call (RPC)
Comments	Supports Microsoft's Network Monitor

Service name	NtLmSsp
Display name	NT LM Security Support Provider
Description	Provides security to remote procedure call (RPC) programs that use transports other than named pipes.
Default startup mode	Manual (Stopped)

Service name	SysmonLog
Display name	Performance Logs and Alerts
Description	Configures performance logs and alerts.
Default startup mode	Manual (Stopped)

Service name	PlugPlay
Display name	Plug and Play
Description	Manages device installation and configuration and notifies programs of device changes.
Default startup mode	Automatic
Dependent services	Fax Service, Smart Card, Telephony, Remote Access Auto Connection Manager, Remote Access Connection Manager, and Internet Connection Sharing

Service name	Spooler
Display name	Print Spooler
Description	Loads files to memory for later printing
Default startup mode	Automatic
Depends on	Remote Procedure Call (RPC)
Dependent services	Fax Service
Comments	Even if the server is not a print server and doesn't send print jobs, it is not recommended to disable the service because it may interfere with future hotfix/Service Pack applications. If changed, best if set to Manual.

Service name	ProtectedStorage
Display name	Protected Storage
Description	Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services, processes, or users.
Default startup mode	Automatic
Depends on	Remote Procedure Call (RPC)

Service name	RSVP
Display name	QoS RSVP
Description	Provides network signaling and local traffic control setup functionality for QoS-aware programs and control applets.
Default startup mode	Manual (Stopped)

Service name	RasAuto
Display name	Remote Access Auto Connection Manager
Description	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.
Default startup mode	Manual (Stopped)
Depends on	Remote Access Connection Manager, Telephony, Plug and Play, and Remote Procedure Call (RPC)

Service name	RasMan
Display name	Remote Access Connection Manager
Description	Creates a network connection.
Default startup mode	Manual (Started)
Depends on	Telephony, Plug and Play, and Remote Procedure Call (RPC)
Dependent services	Internet Connection Sharing and Remote Access Auto Connection Manager

Service name	RpcSs
Display name	Remote Procedure Call (RPC)
Description	Provides the endpoint mapper and other miscellaneous RPC services.
Default startup mode	Automatic
Dependent services	COM+ Event System, System Event Notification, Distributed Link Tracking Client, Distributed Link Tracking Server, Distributed Transaction Coordinator, Fax Service, File Replication, Indexing Service, IPSEC Policy Agent, Kerberos Key Distribution Center, Messenger, mr2kserv, Network Connections, NMS Service, Print Spooler, Protected Storage, Removable Storage, Routing and Remote Access, Task Scheduler, Telephony, Remote Access Connection Manager, Remote Access Auto Connection Manager, Internet Connection Sharing, TlntSvr, and Windows Management Instrumentation
Comments	Opens port 445

Service name	RPCLocator
Display name	Remote Procedure Call (RPC) Locator
Description	Manages the RPC name service database.
Default startup mode	Manual (Stopped)
Depends on	Workstation

Service name	RemoteRegistry
Display name	Remote Registry Service
Description	Allows remote registry manipulation.
Default startup mode	Automatic
Comments	Leaving this set to Automatic is a judgement call. Currently Midwest Bank does use this service on occasion for remote administration.

Service name	NtmsSvc
Display name	Removable Storage
Description	Manages removable media, drives, and libraries.
Default startup mode	Automatic
Depends on	Remote Procedure Call (RPC)

Service name	RemoteAccess
Display name	Routing and Remote Access
Description	Offers routing services to businesses in local area and wide area network environments.
Default startup mode	Disabled
Depends on	NetBIOS Group and Remote Procedure Call (RPC)
Comments	Normally only used on RAS servers.

Service name	seclogon
Display name	RunAs Service
Description	Enables starting processes under alternate credentials.
Default startup mode	Automatic

Service name	SamSs
Display name	Security Accounts Manager
Description	Stores security information for local user accounts.
Default startup mode	Automatic
Dependent services	Distributed Transaction Coordinator and Intersite Messaging

Service name	lanmanserver
Display name	Server
Description	Provides RPC support and file, print, and named pipe sharing.
Default startup mode	Automatic
Dependent services	Backup Exec Remote Agent for Windows NT/2000, Computer Browser, Distributed File System

Service name	SCardSvr
Display name	Smart Card
Description	Manages and controls access to a smart card inserted into a smart card reader attached to the computer.
Default startup mode	Manual (Stopped)
Depends on	Plug and Play

Service name	SCardDrv
Display name	Smart Card Helper
Description	Provides support for legacy smart card readers attached to the computer.
Default startup mode	Manual (Stopped)

Service name	SNMP
Display name	SNMP Service
Description	Includes agents that monitor the activity in network devices and report to the network console workstation.
Default startup mode	Automatic
Depends on	Event Log
Comments	Agent, Traps, and Security parameters are set in the SNMP service's properties. Install this service before installing Dell SNMP utilities.

Service name	SNMPTRAP
Display name	SNMP Trap Service
Description	Receives trap messages generated by local or remote SNMP agents and forwards the messages to SNMP management programs running on this computer. Automatically installed when the SNMP service is installed.
Default startup mode	Manual (Stopped)
Depends on	Event Log

Service name	SENS
Display name	System Event Notification
Description	Tracks system events such as Windows logon, network, and power events. Notifies COM+ Event System subscribers of these events.
Default startup mode	Automatic
Depends on	COM+ Event System

Service name	Schedule
Display name	Task Scheduler
Description	Enables a program to run at a designated time.
Default startup mode	Automatic
Depends on	Remote Procedure Call (RPC)
Comments	Windows NT's at scheduler command is also supported.

Service name	LmHosts
Display name	TCP/IP NetBIOS Helper Service
Description	Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.
Default startup mode	Automatic

Service name	TapiSrv
Display name	Telephony
Description	Provides Telephony API (TAPI) support for programs that control telephony devices and IP based voice connections on the local computer and, through the LAN, on servers that are also running the service.
Default startup mode	Manual (Started)
Depends on	Plug and Play and Remote Procedure Call (RPC)
Dependent services	Fax Service, Remote Access Auto Connection Manager, Remote Access Connection Manager, and Internet Connection Sharing

Service name	TlntSvr
Display name	Telnet
Description	Allows a remote user to log on to the system and run console programs using the command line.
Default startup mode	Automatic, by disabled by template
Depends on	Remote Procedure Call (RPC)
Comments	This has been disabled by the w2kbase security template.

Service name	UPS
Display name	Uninterruptible Power Supply
Description	Manages an uninterruptible power supply (UPS) connected to the computer.
Default startup mode	Manual (Stopped)

Service name	UtilMan
Display name	Utility Manager
Description	Starts and configures accessibility tools from one window.
Default startup mode	Manual (Stopped)

Service name	MSIServer
Display name	Windows Installer
Description	Installs, repairs and removes software according to instructions contained in .MSI files.
Default startup mode	Manual (Stopped)

Service name	WinMgmt
Display name	Windows Management Instrumentation
Description	Provides system management information.
Default startup mode	Automatic
Depends on	Remote Procedure Call (RPC)
Comments	Allows system information to be extracted remotely via VBScript. By default, if the service fails the OS will try to restart the service three times.

Service name	Wmi
Display name	Windows Management Instrumentation Driver Extensions
Description	Provides systems management information to and from drivers.
Default startup mode	Manual (Started)

Service name	W32Time
Display name	Windows Time
Description	Sets the computer clock.
Default startup mode	Automatic

Service name	lanmanworkstation
Display name	Workstation
Description	Provides network connections and communications.
Default startup mode	Automatic
Dependent services	Alerter, Backup Exec Remote Agent for Windows NT/2000, Computer Browser, Distributed File System, Messenger, Net Logon, and Remote Procedure Call (RPC) Locator

Table 16

Services associated with Dell servers

Service name	dcstor32
Display name	Dell OpenManage Server Agent
Description	
Default startup mode	Automatic
Comments	

Service name	dcevt32
Display name	Dell OpenManage Server Agent Event Monitor
Description	
Default startup mode	Automatic
Comments	

Service name	VxSvc
Display name	Disk Management Service
Description	(none)
Default startup mode	Automatic
Comments	Supports Array Manager, which replaces Windows 2000's Disk Management snap-in

Service name	ni_nic
Display name	Intel Client Instrumentation for DMI and SNMP
Description	(none)
Default startup mode	Automatic
Comments	Not strictly a Dell-associated service, but installed when an Intel Pro NIC card is present. Many of the Dell servers in Midwest Bank's environment, such as the Dell PowerEdge 1550, have these NICs.

Service name	mr2ksrv
Display name	mr2ksrv
Description	(none)
Default startup mode	Automatic
Depends on	Remote Procedure Call (RPC)
Comments	Dell software that supports Open Manage

Table 17

Application-based services

Service name	TermService
Display name	Terminal Services
Description	Provides a multisession environment that allows client devices to access a virtual Windows 2000 Professional desktop session and Windows-based programs running on the server.
Default startup mode	Disabled
Comments	Even though this service is not installed, it still shows up by default in the Services list. Will not run unless installed.

Service name	SMS Client Service
Display name	SMS Client Service
Description	
Default startup mode	Automatic
Comments	Starts in the context of SMSCliSvcAcct&, which is a user account automatically created through the SMS client installation and placed into the local Administrators group.

Service name	SMS Logon Service
Display name	SMSLogonSvc
Description	
Default startup mode	Automatic
Comments	Starts in the context of SMSLogonSvc, which is a user account automatically created through the SMS client installation and placed into the local Administrators group.

Table 18

Midwest Bank-specific services

Service name	BackupExecAgentAccelerator
Display name	Backup Exec Remote Agent for Windows NT/2000
Description	Increases backup performance of remote Windows NT/2000 systems by compressing the data to be backed up.
Default startup mode	Automatic
Depends on	Server, DHCP Client, DNS Client, TCP/IP Helper Service, and Workstation
Comments	Installed as part of Midwest Bank's standard procedure. This service is necessary for Backup Exec 8.6 Accelerator Agent to function.

Service name	ITAAgent
Display name	Intruder Alert Agent v3.6
Description	(none)
Default startup mode	Automatic
Comments	Installed as part of Midwest Bank's standard procedure. This service is necessary for Information Security-mandated Symantec Intruder Alert 3.6 to function.

Service name	Norton Antivirus Server
Display name	Norton Antivirus Client
Description	(none)
Default startup mode	Automatic
Comments	Installed as part of Midwest Bank's standard procedure. This service is necessary for Information Security-mandated Norton Antivirus 7.5 CE to function.

Service name	DefWatch
Display name	DefWatch
Description	(none)
Default startup mode	Automatic
Comments	Installed as part of Midwest Bank's standard procedure. This service processes new antivirus definition files, and is necessary for Information Security-mandated Norton Antivirus 7.5 CE to function.

Table 18

Last Updated: February 20th, 2018

Upcoming Training

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 Crystal City 2018	**Arlington, VA**	**Jun 18, 2018 - Jun 23, 2018**	**Live Event**
SANSFIRE 2018	**Washington, DC**	**Jul 14, 2018 - Jul 21, 2018**	**Live Event**
SANSFIRE 2018 - SEC505: Securing Windows and PowerShell Automation	**Washington, DC**	**Jul 16, 2018 - Jul 21, 2018**	**vLive**
SANS Boston Summer 2018	**Boston, MA**	**Aug 06, 2018 - Aug 11, 2018**	**Live Event**
SANS Amsterdam September 2018	**Amsterdam, Netherlands**	**Sep 03, 2018 - Sep 08, 2018**	**Live Event**
SANS Network Security 2018	**Las Vegas, NV**	**Sep 23, 2018 - Sep 28, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**