Global Information Assurance Certification Paper

GIAC Certified Windows Security Administrator (GCWN)

Practical Assignment Version 3.1 (revised April 2002)

Securing Windows 2000 File and Print Servers with Security Templates

Tim Neese

January 2003

Table of Contents

Abstract

To assist with implementing common Best Practice measures to improve security on Windows computers, security templates have been developed to automate the configuring of a number of system settings, including password requirements, account lockout behavior, system-use auditing, audit log retention, security-related options, Registry and file permissions and system service configuration. In this paper, a number of popular security templates for Windows 2000 servers are investigated, one is then implemented in a test environment and tested for its application of security settings, impact on system functioning and its effectiveness in addressing a number of security-related concerns.

Introduction

While the computer industry is still relatively young, little more than 50 years old, the last 30 years have seen a dramatic series of developments. The seventies were dominated by mainframe and mini computing environments with centralized systems and only dumb terminals for user interaction. The eighties saw the introduction of mass-marketed standalone personal computers, which while limited in processing power, still ran many personal and business applications. In the nineties, those personal computers became networked and centralized applications became client/server so that processing power and efficiencies could be optimized; servers stored, manipulated and managed data while client desktop computers provided rich graphical interfaces to the system.

As computer systems became interconnected, new challenges have arisen to maintain the security of information systems. These systems are now accessed from a variety of different client computers such as those of employees, external suppliers and customers. These systems often run multiple servers with each server performing different functions such as database servers for data storage, application servers for client/server applications, and web servers for client access from inside or outside a company. While this distribution of processing has enabled systems that can process millions of transactions or service millions of users, each computer, whether client or server, introduces another point of entry to compromise the security of the whole system.

Securing a computer system, whether it is a standalone desktop system or a complex client/server intranet/internet application server cluster, encompasses a broad range of activities. Information security focuses on maintaining the confidentiality, integrity and availability of data stored in information systems by authenticating users to verify that users are who they say they are and by restricting access to only the resources for which a user is authorized to access. [1] (Microsoft TechNet, Best Practices for Enterprise Security) Within an organization, it can include defining and implementing policy to ensure that people are informed and held accountable to appropriate conduct with regard to the use of a computer system. Within the computer system itself, it includes the processes to handle authentication and authorization within that system as well as mechanisms to protect the system against misuse. Within the support of that system it can include activities by staff to monitor and audit that system against possible misuse. Within the maintenance of that system it includes regular measures to fix known and unknown vulnerabilities. When a compromise in the system's security occurs, it includes taking measures to identify what has occurred, by whom and how it occurred as well as restoring the system to its original state before the incident.

While all of these activities are important and necessary to ensure the confidentiality, integrity and availability of a computer system, this paper will focus on one aspect of security: configuring a Windows 2000 server to help prevent that server from becoming compromised and ensuring that adequate security data is gathered to be able to monitor a system for possible misuse. An investigation into

security recommendations for nearly any system often leads one to a checklist of things to do to help improve a system's security such as Best Practice checklists from LabMice [2] (LabMice.net, Windows 2000 Security Checklist) and Microsoft [3] (Microsoft TechNet, Best Practices for Enterprise Security). These include such items as setting rules for accounts and passwords, specifying which events will be logged when using the system, enabling a number of security-related settings on the system and disabling services that are unnecessary for the functioning of the system.

While a checklist provides a good way to call attention to measures that can be taken to reduce the vulnerability of a system, the actual configuration of the system to implement the recommendations must still be completed, which can take a considerable amount of time if done manually and lead to errors if an item is missed or configured incorrectly. Microsoft offers an aid for configuring computer systems through the use of security templates that define a number of system or security-related settings. These templates can also set the permissions on files, directories and registry items to further restrict access to these items.

For this paper, a security template was selected from a number of commonly used templates. This template was applied to a Windows 2000 file server because file servers are found in nearly every business computing environment and often store sensitive, mission-critical information. Furthermore, many organizations have more than one file server, so that keeping the security configuration consistent on these servers poses an additional challenge to system administrators. Within a Windows 2000 network with Active Directory, the Group Policy facility provides a mechanism for automating the implementation of this security template on multiple servers. The Baseline and File and Print Incremental security templates included in the Microsoft Security Operations Guide were then implemented in a test environment and evaluated for their effectiveness and impact on system functionality.

Description of system

Computing environment

For the purposes of applying and evaluating a Windows File Server security template, a test network was constructed with a Windows 2000 Active Directory domain controller; two Windows 2000 file servers and a Windows 2000 Professional workstation.

The domain controller was installed in native mode since it is the sole domain controller. Active Directory was installed without backward compatibility since the client will be a Windows 2000 Professional workstation. This choice for a pure Windows 2000 environment was made because operating AD in mixed mode costs functionality on legacy clients, such as Group Policy, and opens up more security vulnerabilities such as with null session reconnaissance. Windows NT is nearing the end of its supported product-cycle and Windows 9x/Me lacks many essential security elements so that many companies choose to operate Windows

2000 environments alongside older environments and migrate users to the new environment in place of mixing the two. Having legacy clients often results in the negotiation of least-common-denominator security options, which tend to be less secure.

All four machines were installed as virtual machines using the VMware Workstation 3.1 software. This software allows the machines to interact with each other as if they were physical computers connected by an Ethernet network. The Operating System specifications of the four machines are as follows:

TSTDC	Windows 2000 Server with an Active Directory domain in native mode
TSTDATA1	Windows 2000 Server
TSTDATA2	Windows 2000 Server
TSTDesktop123	Windows 2000 Professional

All machines were updated with Windows 2000 Service Pack 3 and all essential security hotfixes as identified by the HFNETCHK tool.

```
Microsoft Network Security Hotfix Checker, 3.32
Copyright (C) Shavlik Technologies, 2001-2002
Developed for Microsoft by Shavlik Technologies, LLC
info@shavlik.com (www.shavlik.com)

Using XML data version = 1.0.1.449  Last modified on 1/10/2003.

Scanning TSTDATA1
.....................................................
Done scanning TSTDATA1
---------------------------
TSTDATA1 (194.10.10.22)
---------------------------

        * WINDOWS 2000 SERVER SP3

        Note            MS01-022        Q296441
        Note            MS02-008        Q318202
        Note            MS02-008        Q318203
        Note            MS02-008        Q317244
        Patch Found     MS02-042        Q326886
        Patch Found     MS02-045        Q326830
        Patch Found     MS02-048        Q323172
        Patch Found     MS02-050        Q329115
        Patch Found     MS02-051        Q324380
        Note            MS02-053        Q324096
        Warning+        MS02-055        Q323255
        Patch Found     MS02-063        Q329834
        Note            MS02-064        Q327522
        Note            MS02-065        Q329414
        Patch Found     MS02-069        810030
        Warning++       MS02-070        309376
        Patch Found     MS02-071        328310

        * INTERNET EXPLORER 5.01 SP3

        Patch Found     MS02-009        Q318089
        Patch Found     MS02-015        Q319182
```

```
  Patch Found     MS02-023        Q321232
  Note            MS02-027        Q323889
  Note            MS02-047        Q323759
  Patch Found     MS02-066        Q328970

+File \\TSTDATA1\C$\WINNT\system32\hhctrl.ocx has a
file version that is greater than what is expected.

++File \\TSTDATA1\C$\WINNT\system32\sp3res.dll has a
file version that is greater than what is expected.
```

[Figure 1: HFNETCHK Output]

Hardware specifications

Because the four virtual machines all reside on the same physical computer, their hardware is identical:

System Manufacturer	VIA Technologies, Inc.
System Model	VT8363
System Type	X86-based PC
Processor	x86 Family 6 Model 6 Stepping 2 AuthenticAMD ~1394 Mhz
Hard Drive	Single 4 GB partition
Network card	Realtek RTL8029(AS) PCI Ethernet Adapter

The memory specifications differ per machine based on the different role that it serves:

TSTDC	192 MB
TSTDATA1	160 MB
TSTDATA1	160 MB
TSTDesktop123	132 MB

The system upon which VMware Workstation 3.1 ran and on which the test environment was constructed was as follows:

OS Name	Microsoft Windows XP Professional
Version	5.1.2600 Service Pack 1 Build 2600
OS Manufacturer	Microsoft Corporation
System Manufacturer	VIA Technologies, Inc.
System Model	VT8363
System Type	X86-based PC
Processor	x86 Family 6 Model 6 Stepping 2 AuthenticAMD ~1394 Mhz
BIOS Version/Date	Award Software International, Inc. 6.00 PG, 11-3-2002
SMBIOS Version	2.3
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\System32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Time Zone	W. Europe Standard Time
Total Physical Memory	768,00 MB
Total Virtual Memory	2,21 GB
Page File Space	1,46 GB
Hard drive	60 GB 7200 RPM Western Digital ATA-133
Network card	Realtek RTL8029(AS) PCI Ethernet Adapter

Additional software and hardware

McAfee Netshield version 4.5 Service pack 1 Hotfix rollup 1 was installed on the three Windows 2000 Server machines with the latest scan engine, version 4.1.60, and the latest antivirus DAT files available at the time of testing, 4.0.4242. McAfee VirusScan version 4.5.1 Service Pack 1 was installed on the Windows Professional workstation, TSTDesktop123, with scan engine 4.1.60 and version 4.0.4242 DAT antivirus definitions.

Microsoft Terminal Server was also installed on the three Windows 2000 Server machines for remote administration purposes. The Terminal Services Client from Microsoft was then installed on the TSTDesktop123 workstation.

Since this is a test environment, backup has not been arranged for these servers. In practice this would done either with software such as ArcServe and a tape backup drive or Tivoli Storage Management software and a tape robot. In the case of this test, copies of the virtual machine images were made to ease restoring a particular system state if needed.

The test network is situated behind a firewall which does not allow any incoming traffic to any of the test machines since there are no public web servers or email servers which must be contacted from outside of the network. The network is connected to the Internet via an Alcatel SpeedTouch ADSL Ethernet modem which is configured as a router. The routing table on the ADSL modem is set to forward all incoming traffic to the computer on which all of the virtual machines in the test network run. This host uses Zone Alarm Personal with a firewall configuration of High for the Internet zone and Medium for the Trusted zone.

System role and security requirements

This paper investigates the use of a security template to improve the security on a Microsoft Windows 2000 File or Print server. The role of this server can be understood by identifying the function it performs in a company's computing environment, the way it will be accessed and the expectations that users have of that server. For a given role, a number of threats to the security of that server can be identified. To best address these threats, a number of security requirements can then be identified to assist in selecting measures to secure a system.

Throughout this paper the term "file server" will be used to describe a server which offers storage of computer data and printer queues. Depending on a company's size, these functions may be offered on one server or split across dedicated servers: one for file sharing and one for printing. In larger computing environments, one often finds a combination of multiple dedicated and dual-use file/print servers: dedicated servers for broad usage and dual-use servers for specialized purposes such as departmental servers.

Regardless of this, the general role of a file or print server shares a number of aspects. This server functions as a central data storage resource and in the case

of a print server, provides a central queuing facility for printing. A file server is generally only accessible from within the company's network or via a company's dialup facilities. Since a computer user often already has local storage space on his or her desktop computer, a file server provides a storage space for data that can be access from multiple locations within the network either by one individual as in the case of one's home directory, or to share data with others as in the case of shared data or application directories. Similarly, while a print queue can be created on one's own desktop computer, doing so on a central server allows that printer to be used by multiple people. Users of both resources have an expectation of a very high level of availability from the resource as down-time results in missed work-time or could result in loss of critical documents or data.

Networked access brings with it significant threats to a file server since it must be accessible from most computers on a company's network because it serves as a central data storage resource. This is a threat because it can be difficult to control what is running on the computers of the users accessing the file server. For example, a number of viruses carry key-logging payloads that capture passwords as they are typed and email them back to a central location. While this is more generally a threat to the authentication on a network, it affects file servers because compromising the password for an account gives one access to the resources on a server for which that account is authorized to access. Furthermore, the communication between one's client computer and a file server could be intercepted over the network and either inspected for sensitive data or replayed in a man-in-the-middle attack.

Reconnaissance activity poses another threat to servers on a network, and file servers in particular. Windows servers can allow unauthorized users, so called null sessions, to connect to a server and read specific information about that server which includes items such as the groups and accounts on that server, data shares offered on that server, operating system type, account policy information, etc. While this functionality is used by some applications, malicious users could scan a network to map out which servers store desirable information to target their hacking attempts or use null session connections to shares for brute-force password cracking attempts. As Eric Cole notes in his book, Hackers Beware,

> "In addiction to potentially giving away user information though null sessions or Registry edits, and the potential loss of data from unsecured shares, null sessions also allow certain new viruses to spread rapidly throughout a network." [4] (Cole, p.437)

Misuse of authorization on a file server poses another significant threat. This misuse can through various means: one, to compromise another person's account and password to gain access to data directories for which one is not approved to access and the other is to elevate one's user rights on the file server itself to be able to perform functions on the server that otherwise would not be possible such as installing a service.

File servers store confidential information such as company personnel records, accounting reports, meeting notes, Research & Development designs, project documentation, etc. Windows controls access to items by means of discretionary access control lists (DACLSs) that are set on every file, folder and registry item on Windows servers which then include lists of security identifiers from local and domain (network) groups and user accounts. If you can log in with someone else's account, then you could gain access to data that your account would not be able to access.

Since limitations are often set on what a regular user can do on a server, such as not being able to install software, modify a server's system configuration, etc., another threat is the elevation of one's privileges to be able to perform such tasks. This could be used to render the server inoperable, delete data or install software to use the server as a staging base for further hacking or attacks on other networked computers.

Finally, since some accounts on a server such as Administrator and LocalSystem have special privileges giving them access to everything on the server, one could try to discover the password of the Administrator account or install software that ran within the security context of the LocalSystem account to gain access to all of the data stored on that server. Although this is always a serious breach in security on a server, on a file server it effectively circumvents all of the authorization controls to the data stored on that server.

The security requirements then of a file server should address these threats. In terms of account and password policies, a file server should provide a minimum level of security but may not need to use the most stringent possible policies since users will typically use a domain account to access that server instead of local accounts. Authentication on a Windows 2000 network occurs between the client computer and domain controller computers. When a user attempts to access something on the server, the security identifiers for the groups to which he or she is authorized are checked by the file server against the DACLs set on the files, directories and registry items to determine if he or she is permitted access. Therefore, for a network account, a more stringent account and password policy is necessary on the domain controller. Local accounts on a file server are generally not used for giving access to the data stored on that server or to access that server. While additional account and password requirements would not hurt, a minimum level of requirements should be acceptable for a file server.

Since a number of people will be accessing the server from a variety of client computers, recording information about attempts to access the file server and the resources on it is very important for monitoring and diagnosing possible misuse of privileges or resources on the server. Windows 2000 offers a rich set of possibilities for recording events relating to logon, account management, access of data, privilege use, policy changes, process tracking and system events to name a few. Additionally, events are recorded in a server's application and system logs

from applications and the operating system on that server. These logs are crucial for being able to track activity, both normal and possible misuse, on a server. Adequately configuring what information will be logged and configuring options for these logs is an important security requirement on a file server, as it is for all servers on a company's network.

Since a file server holds confidential documents or data which are critical to a company's business, additional steps should be taken to protect a file server against possible misuse, both from the network or at the server's location should someone gain physical access to the server. Windows provides a host of additional settings to enforce more secure network communication with the server in the form of packet signing and secure channel encryption, clearing of virtual memory page files when the sever is shut down, deleting of cached logon credentials when the server is shut down, restricting anonymous access to the server, etc., to name but a few. To the extent that these extra settings do not impede normal functioning of the server, they can be activated to better help prevent misuse of the server or its resources.

Since many vulnerabilities of computer systems exist as a result of a unintentional use of program functionality or flaws in that software's code, disabling unnecessary software on a file server also further protects against unknown exploits of potential vulnerabilities. Software that runs as a service on a server is particularly vulnerable since it often runs with the privileges of the LocalSystem account, which has access to everything on the server, and often accepts connections from the network. While this is not true for every service on a server, disabling unnecessary services is a good preventative measure for protecting a server against attack. Thus, a final security requirement for a file server would be to disable system services that are not required for the operation of the file server.

Selection of Template

Investigation of available templates

Searching for possible security templates that would be appropriate for a company's file or print server began with Microsoft itself. Windows 2000 Server comes with a number of standard security templates for workstations and servers. Of these, the Basic, basicsv.inf, Secure, securews.inf, and HighSecure, hisecws.inf, templates can be used to configure password, account lockout, audit, user right assignment, security options, Event Log, Restricted Groups, System Services and File and Registry permissions. In addition to these, Microsoft offers more security templates in its Security Operations Guide. Of these, the baseline.inf and File and Print Incremental.inf are relevant for file servers. As part of its Security Benchmarks and Scoring Tools, the Center for Internet Security has also developed a Windows 2000 Level I security template, CIS-Win2K-Level-I-v1.1.7.inf, which incorporates many of the security Best Practices published by the SANS Institute, the National Security Agency, the United States Department of Defense and the Center for Internet Security. Additionally, the National Security

Agency provides a template, w2k_server.inf, with its Microsoft Windows 2000 Network Architecture Guide. These six templates were included in the selection process for this paper.

These templates could be used to configure more than 100 settings on a Windows 2000 server. Often they include a subset of the possible settings, leaving some items unchanged from a default Windows 2000 server installation. While templates thought to be more secure do indeed configure more settings, they can also miss ones that one might expect to be included or configure options so stringently that a server only works in specific computing environments or performs poorly as a result of extra processing required by the security configuration. Even after reading the documentation supplied with many of the templates to explain the features being configured and the security principles the changes are intended to address, selecting a template can be very difficult. This selection must balance the security requirements of one's computing environment with the impact that implementing that configuration will have on server performance and maintenance.

Selection criteria

Security templates are used to configure a set of configuration options and permissions on a Windows server. That server, in turn, is part of a larger collection of servers on a company network which includes other servers for services such as logon authentication. The network also includes the client computers that access this server. Finally the computers on the network are used to facilitate business processes. Because computer security involves a complex mix of technical and organizational measures to ensure the confidentiality, integrity and availability of information, and because the configuration of security settings on a server addresses only a small part of possible security measures, a security template can not be evaluated solely on whether or not it make a server "secure". A security template can best be evaluated on what it adds to a computer's present configuration.

These settings, however, come at a price. A setting that enforces a higher level of security can make a system inaccessible to certain client computers, cause some software to not function correctly or require extra maintenance of the server. These trade-offs will be discussed in depth when relevant for given security settings but the consequences of security-related settings are important to determining a template's suitability.

As is the case with any kind of template, security templates are used to provide a standard approach to implementing a particular task and to incorporate desired practices to be followed when completing that task, whether composing a common business document or in this case, server configuration. Security templates that are used to configure security settings on servers should then incorporate a variety of Best Practices from the field of information security such as enforcing particular account policies when relevant, ensuring that adequate information is logged in the

use of that server, enable options to prevent misuse of that server's resources and disabling unused services on that server.

Therefore, the selection criteria for choosing a security template is the extent to which a template's settings contribute to implementing Best Practice recommendations with an acceptable level of impact on the performance or functionality of the system to which it is applied.

Selection methodology

To assist with selecting a template from the six security templates mentioned above, a table was created with all of account, auditing, user right assignment, security options, event log, restricted groups and system services included in each template, as well as those present with a default installation of Windows 2000 Server.

This information was gathered using the Security Configuration and Analysis Microsoft Management Console Snap-In on the TSTDATA1 server after its default installation. Each template was imported into its own security database and then this database was analyzed to compare those settings with those of the server. This server was a member of the Computers Organizational Unit in the Active Directory with only a standard default domain policy active at that time. Each window pane in the console was exported to a text file and then copied into a Excel spreadsheet to produce the table in Appendix A. Security Template Security Setting Comparison. Seeing each template side by side did not simplify the selection task as each template included some options that could be desirable and missed others. A method was needed to be able to assign priority and cost, in terms of implementing and maintaining the configuration, to each of the configuration items and to compare templates with each other.

The list of configuration items was then copied to a second worksheet and given a score of 0-5 with 5 offering the most added security relative to the default setting with the least negative impact for implementing that setting. A score of 0 was given to items that were the same as the default configuration. Thus a security setting that added more security to an important setting with little negative impact would receive a higher score than one that added similar extra security but at a higher impact for implementing that setting This was particularly evident with the maximum size of the event logs, which in one template were set to 4 GB, which would require taking care that the disk where the logs are stored was sufficiently large to prevent that the disk would fill up and disrupt use of the server or , in combination with other settings, automatically shut the server down. When settings were sufficiently related to each other, such as with account, audit and user right assignment settings, these were grouped into one item to be scored. These scores were then totaled as shown in Appendix B. Security Template Selection Scoring. The template with the highest score was selected as offering the most additional security given the impact of implementing the template.

The Baseline and File and Print Server Incremental security templates from the Microsoft Security Operation Guide received the highest score with a total of 71 points. This does not change, however, the inherent trade-off to the additional security and the impact that it poses to implementing it. While this template provides a number of important additions to a server's security, it also does so at a price to its ease of implementation. However following a principle of starting with a more restrictive configuration and relaxing it as needed, this template appears a good choice for some Windows 2000 network environments.

Template Elements

Since the security templates were evaluated on the basis of what they added to the server's default configuration, the security settings from the Microsoft Baseline templates will be listed next to the default security settings to provide a better view of what settings the template changes relative to the default values. The impact of a particular setting's value will be discussed in the evaluation of the template. The settings are grouped by the categories used in the Security Configuration and Analysis (SCA) MMC Snap-In. They were extracted using the SCA MMC Snap-In on the TSTDATA1 server following a clean install of the operating software, service pack 3, necessary OS security hotfixes and antivirus software.

Password and Account Lockout Policy

	Default Computer Setting	MS Baseline Template
Enforce password history	0 passwords remembered	Not defined
Maximum password age	42 days	Not defined
Minimum password age	0 days	Not defined
Minimum password length	0 characters	Not defined
Passwords must meet complexity requirements	Disabled	Not defined
Store password using reversible encryption for all users in the domain	Disabled	Not defined
Account lockout duration	Not defined	Not defined
Account lockout threshold	0 invalid logon attempts	Not defined
Reset account lockout counter after	Not defined	Not defined

These two groups of policies influence, among other things, frequency, complexity and uniqueness of passwords that are required for either network or local accounts. The account lockout policy specifies after how many failed logon attempts an account is locked out and for how long. When these account policies are set using the Active Directory Domain Security Policy tool, then they apply to the domain account. When they are set on a Group Policy object for an AD Organizational Unit, then they apply to the local account on machines in that OU. These policies can also be configured using the Local System Policy console on servers not in an OU with a Group Policy policy to set these settings, however Group Policy polices linked to a site, domain or Organizational Unit will override these local policies.

Weak passwords are on of the most prevalent causes of security compromises since these can be easily guessed, sniffed or cracked, as is indicated by its position of number seven for Windows computers on the SANS/FBI Top 20 vulnerabilities list. [5] (SANS Institute, The Twenty Most Critical Internet Security Vulnerabilities) One must be careful, however, that the password policy doesn't cause users to write down their passwords or follow easy to guess password naming cycles out of frustration from the more stringent requirements.

These password policies should also be implemented appropriately for the method of access to resources. Network accounts will typically have the most requirements, servers, such as application servers which make use of local accounts, may implement some level of password complexity while other servers that do not have local accounts other than the built-in accounts may not need additional password policies beyond the default settings. As indicated here, the Microsoft Baseline security template does not change the default password and account policies, since these must be modified to fit the security requirement of the servers to which the template will be applied.

Audit Policy

	Default Computer Setting	MS Baseline Template
Audit account logon events	No auditing	Success, Failure
Audit account management	No auditing	Success, Failure
Audit directory service access	No auditing	Failure
Audit logon events	No auditing	Success, Failure
Audit object access	No auditing	Success, Failure
Audit policy change	No auditing	Success, Failure
Audit privilege use	No auditing	Failure
Audit process tracking	No auditing	No auditing
Audit system events	No auditing	Success, Failure
Event Log Policy		
Maximum application log size	512 kilobytes	10240 kilobytes
Maximum security log size	512 kilobytes	10240 kilobytes
Maximum system log size	512 kilobytes	10240 kilobytes
Restrict guest access to application log	Disabled	Enabled
Restrict guest access to security log	Disabled	Enabled
Restrict guest access to system log	Disabled	Enabled
Retain application log	7 days	Not defined
Retain security log	7 days	Not defined
Retain system log	7 days	Not defined
Retention method for application log	By days	Manually
Retention method for security log	By days	Manually
Retention method for system log	By days	Manually
Shut down the computer when the security audit log is full	Disabled	Enabled

These settings control what activity will be logged to the security log on the server and they control the configuration of the Applications, Security and System logs. Collecting and analyzing log information is one of the most valuable tools in monitoring unauthorized activity and conducting forensic analysis when a security incident occurs. Auditing both Success and Failure events for account logon

events and logon events generates event log entries for both local and network connections to the server. This can be useful for detecting null session scan activity and brute-force password-cracking attacks to guess passwords by connecting repeatedly to file shares. Auditing Success and Failure of the object access item logs events whenever there is an attempt to access a file, directory or registry key for which a system access control list (SACL) has been enabled for object access auditing. Setting this at the server level enables this logging but it must also be set for each object where the auditing is desired. Auditing of Policy Change events generates events whenever a local system policy on the server is modified which is useful to track changes in the local system policy on a server, especially sine changing this policy could be done to prevent suspicious activity from being logged. The auditing of Failures with Privilege Use helps to identify attempts by users to exercise User Rights for which they are not authorized such as accessing the security log. With this template's setting to audit Success and Failure of System Events, log entries will be generated when the server shuts-down/restarts or when there are events that affect system security or the security log.

The Event log policies control the behavior of the Windows Event log which stores the events generated by auditing policies in the Security log, events from software in the Applications log and by the Operating system in the System log. The size set here is important; if these are larger than the available disk space on the hard drive where the logs are stored, the drive will fill up and can cause a disruption in service. If they are stored on the same drive as the operating system, and there is insufficient available drive space to accommodate the maximum log size, then this is a Denial of Service attack waiting to happen.

Another important setting for the Event logs is the Restrict Anonymous access. While this access is normally only read level to the Applications and System log (access to the Security log requires an additional user right), this setting prevents anonymous and null session connection from any access to the logs.

Retention of the logs determines when events will be overwritten. The default is to not overwrite events until they are more than 7 days old as specified by both that events are retained for 7 days and that the retention method is set to By Days. With this retention method, one should ensure that the maximum log size is large enough to accommodate the number of events generated in the given number of days. When this retention method is set to Manually, then is Event logs must be cleared manually before events can be logged, should the log reach its maximum size. In combination with other security settings, this can result in a system being automatically shut down. This can be desirable from a security standpoint since some hacking activities can generate unusually large numbers of security events. One of these options is configured in this section, "Shut down the computer when the Security audit log is full" but there is also a Security Option to "Shut down system immediately if unable to log security audits." System administrators need to

ensure that they monitor these logs closely if the retention method is set to Manually.

User Rights Assignment Policy

	Default Computer Setting	MS Baseline Template
Access this computer from the network	Backup Operators,Power Users,Users,Administrators,Everyone	Not defined
Act as part of the operating system		Not defined
Add workstations to domain		Not defined
Back up files and directories	Backup Operators,Administrators	Not defined
Bypass traverse checking	Backup Operators,Power Users,Users,Administrators,Everyone	Not defined
Change the system time	Power Users,Administrators	Not defined
Create a pagefile	Administrators	Not defined
Create a token object		Not defined
Create permanent shared objects		Not defined
Debug programs	Administrators	Not defined
Deny access to this computer from the network		Not defined
Deny logon as a batch job		Not defined
Deny logon as a service		Not defined
Deny logon locally		Not defined
Enable computer and user accounts to be trusted for delegation		Not defined
Force shutdown from a remote system	Administrators	Not defined
Generate security audits		Not defined
Increase quotas	Administrators	Not defined
Increase scheduling priority	Administrators	Not defined
Load and unload device drivers	Administrators	Not defined
Lock pages in memory		Not defined
Log on as a batch job		Not defined
Log on as a service		Not defined
Log on locally	Backup Operators,Power Users,Users,Administrators,STST01DA001\Guest, STST01DA001\TsInternetUser	Not defined
Manage auditing and security log	Administrators	Not defined
Modify firmware environment values	Administrators	Not defined
Profile single process	Power Users,Administrators	Not defined
Profile system performance	Administrators	Not defined
Remove computer from docking station	Power Users,Users,Administrators	Not defined
Replace a process level token		Not defined
Restore files and directories	Backup Operators,Administrators	Not defined
Shut down the system	Backup Operators,Power	Not defined

	Users,Administrators	
Synchronize directory service data		Not defined
Take ownership of files or other objects	Administrators	Not defined

While discretionary access control lists (DACL's) on files, directories and registry keys give users access to objects on a server, user rights allow users to perform particular functions on a computer. This ranges from being able to log in either locally or remotely to a machine, performing backup and restores operations, shutting down the system, managing various aspects of a computer's operation and more. It's precisely the difference in how these rights are assigned along with permissions assigned to the default local groups on a computer that delineates the difference in functionality between the built-in groups of Administrators, Backup Operators, Power Users and regular Users. While many security templates do not change the defaults user rights assignments, there are some security Best Practice recommendations to be more restrictive, especially regarding the Backup and Restore rights as these can be used in combination to circumvent the NTFS permissions on a server. Since remote administration from servers is often the most practical way to administer servers in secured locations, restricting the Log on Locally right to only the Administrators group or other system admin staff is important. On servers that make use of Terminal Server or Citrix for application sharing, then this right could also be given to a group with the users authorized to log into that server including the TSInternetUser account as needed. This account is not needed for use of Terminal Services for remote administration and can best be disabled. The NSA security template was the only one of the templates investigated that was more restrictive with the assignment of these user rights relative to a default installation.

Security Options Policy

Since many Security options are left unchanged by the Microsoft Baseline template, only the options that play a more significant role in securing a Windows 2000 file or print server will be highlighted here.

Security Option	Default Setting	MS Baseline Template	Comments
Additional restrictions for anonymous connections	None. Rely on default permissions	No access without explicit anonymous permissions	Windows servers allow one to connect to a server with an account which has no authorization to access that server, a so called null session, and read information about that server such as operation system, local accounts/groups and shares. This information can be useful to people searching for servers on a network as possible targets of an attack. This setting helps to prevent these connections or limit the information that is available to a null session. It can disrupt the functioning of some applications or with multi-domain trusts. [6] (Microsoft, Microsoft Knowledge Base Article - 246261) This restriction, however, only applies to unauthenticated accounts. Regular domain or local user accounts could still read this information and, thus, could still be used for reconnaissance on a company's network.
Allow Automatic Administrator Logon	Not defined	Not defined	This option allows the server to automatically log in with a given account and password when booted. It is not recommended since the password is stored in the Registry in clear text and could be read by an intruder if not properly secured with permissions.
Allow system to be shut down without having to log on	Disabled	Disabled	Not enabling this option helps to ensure that only authorized users would be able to shut down a server, both by ensuring that the person logging in had the Log on locally and the Shut down the system user rights.
Audit use of Backup and Restore privilege	Disabled	Disabled	Since the Backup and Restore rights can be used in combination on the same account to bypass the NTFS rights on a file, then this option enables logging on backup/restore activity. It generates, however, a very large amount of events, so it is often not practical for servers with large amounts of files that are being backed up.
Automatically log off users when logon time expires (local)	Enabled	Enabled	If times are specified that a user account is allowed to connect to the server, then this option disconnects session that exceed that logon time which helps to ensure that people do not remain connected outside of their authorized time windows.

Security Option	Default Setting	MS Baseline Template	Comments
Clear virtual memory pagefile when system shuts down	Disabled	Enabled	Computers store frequently used information in a memory page file(s) on disk. When the system is shut down the physical memory is cleared but this page file remains on disk. If the hard disk were stolen, this file could be read and analyzed to extract sensitive information that was stored in the page file during server operation. This option deletes this file when the system shuts down. This does not, however, prevent someone from forcing a crash of the system and causing it to shutdown unexpectedly without deleting this file
Digitally sign client communication (always)	Disabled	Disabled	These four options control the digital signing of the Server Message Block (SMB) packets between clients and the server and between the server. This signing of the packets helps to ensure that the packets being received are in fact the same ones that were sent by the client or server sending them. This is to prevent the interception and replaying of these packets as a way of intercepting data being sent between the two computers. Since this traffic is not encrypted however, this option only helps to ensure the authenticity of the packet-sender. It does place a 10-15% processing burden on the computers. Since the Baseline template requires that server communications always be signed, clients that are not capable of doing so will not be able to connect to resources on a server with this policy. Windows 2000 and higher computers as well as Windows NT with Servicepack 3 or higher are capable of digitally signing SMB packets.
Digitally sign client communication (when possible)	Enabled	Enabled	
Digitally sign server communication (always)	Disabled	Enabled	
Digitally sign server communication (when possible)	Disabled	Enabled	
Disable Media Autoplay	Not Available	All Drives	When CD-ROMs are inserted into a drive, a file can be opened automatically on the CD-ROM to ease software installation or the playing of media files. This feature could be misused to automatically launch a malicious program such as a computer virus or other malicious program.
Do not display last user name in logon screen	Disabled	Enabled	When someone logs in locally to a computer, the name of the last user to have logged into that machine is displayed in the logon dialog box. Security Best Practice guidelines often suggest disabling this to reduce disclosing account names that could later be used in password cracking attempts.

Security Option	Default Setting	MS Baseline Template	Comments
LAN Manager Authentication Level	Send LM & NTLM responses	Send NTLMv2 response only\refuse LM & NTLM	Windows computers can use a variety of protocols for authenticating for network logons. These include LanManager, NTLM 1, NTLMv2 and Kerberos. Computers with Windows 2000 or newer will authenticate using Kerberos when logging on via a Windows 2000 domain controller, but older operation system such as Windows NT or Windows 9x/Me clients could use LanManager, NTLM or NTLMv2. Of these, NTMLv2 offers the strongest level of security. While it is supported on Windows 2000 and higher clients, it's also supported on Windows NT 4.0 computers with Service pack 6 and Windows 9x/Me clients with the Active Directory Services client. [7] (Microsoft, Microsoft Knowledge Base Article - 239869) It is one of the options that will help to reduce the risk of passwords being intercepted over the network and decoded. Even if a network does not contain legacy clients, this option ensures that an insecure authentication method such as LanManager is not negotiated, which could happen for example if Kerberos authentication failed, since only NTMLv2 response will be sent or accepted.
Message text for users attempting to log on			These two options allow a custom message and window title to be displayed on the logon dialog box when users press the CTR-ALT-DEL keys to logon. Such a statement is often recommended as a way of keeping users apprised of the most important points of appropriate-use policies. Although this can also be done with logon scripts or by other means, these options display this message before a user logs on.
Message title for users attempting to log on			
Number of previous logons to cache (in case domain controller is not available)	10 logons	0 logons	When a user logs off of a Windows 2000 computer, his or her logon credentials can be stored locally in a cache so that should the computer be unable to communicate with the domain controller, he or she would still be able to log in using these cached credentials. Of course anything that is stored locally could be compromised should someone gain access to the hard drive either physically or remotely. In the event of network failure, then one could still log in with the local account such as Administrator. On laptop computers this could be set to 1 to allow a user to log on to his or her laptop without a network connection but with servers this is not necessary.
Prevent users from installing printer drivers	Enabled	Enabled	This option allows only Administrators and Power Users to install a printer driver. As printer drivers could be modified to include a Trojan horse program, it is often recommended to restrict this on servers.

Security Option	Default Setting	MS Baseline Template	Comments
Rename administrator account	Administrator	Not defined	These two options allow the two built-in accounts, Administrator and Guest to be renamed. Since these accounts are always created on Windows NT and newer computers, people have two accounts to target with hacking attempts. Since the SIDs of the built-in Administrator and Guiest accounts are well known, people remain divided as to whether the protection gained by renaming these accounts is worth the added maintenance of doing so. In addition to renaming the accounts, though, the default description should also be changed. Some people create a dummy Administrator account with no privileges to throw hackers off track. This is left unchanged in the Baseline template.
Rename guest account	Guest	Not defined	
Restrict CD-ROM access to locally logged-on user only	Disabled	Enabled	These two options are designed to prevent others from accessing the floppy or CD-ROM drives from across the network while someone is logged on locally to a computer. If no one is logged on locally, then these drives can be access from the network. On a server, this offers a little extra protection.
Restrict floppy access to locally logged-on user only	Disabled	Enabled	
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled	Enabled	Instead of allowing the security options of Secure Channel communications to be negotiated, the first option ensures that Secure Channel packets will be signed or encrypted. When a computer is booted, it uses its computer account password to create a Secure channel connection to the Domain controller through which things such as NTML pass through authentication and SID/Name lookups are performed. The integrity and encryption of this communication is also important to preventing man-in-the-middle attacks (via packet signing) or network sniffing (via data encryption) to intercept passwords. The last option can be used to ensure that a 128-bit key is used when encrypting Secure channel communication to strengthen the security of this data.
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled	Enabled	
Secure channel: Digitally sign secure channel data (when possible)	Enabled	Enabled	
Secure channel: Require strong (Windows 2000 or later) session key	Disabled	Enabled	
Shut down system immediately if unable to log security audits	Disabled	Enabled	This option is intended to prevent a system from operating when security events can not be logged. However, if the log size and retention method are not set to adequately handle the normal number of security events logged within the retention cycle or maximum log size, then this option could cause a server to shut down when there is no security incident.
Unsigned driver installation behavior	Warn but allow installation	Do not allow installation	These two options configure whether or not the installation of drivers or other software that is not digitally signed will be permitted to not. Since there are still a number of drivers, especially printer drivers that are not signed, configuring this setting too strictly can impede server operation.
Unsigned non-driver installation behavior	Silently succeed	Warn but allow installation	

System Services Policy

	Default Computer Setting		MS Baseline Policy	
	Status	Startup Type	Status	Startup Type
Alerter	Started	Automatic		Disabled
Application Management		Manual		Disabled
Automatic Updates	Started	Automatic	Started	Not Defined
Background Intelligent Transfer Service		Manual		Not Defined
ClipBook		Manual		Disabled
COM+ Event System	Started	Manual	Started	Manual
Computer Browser	Started	Automatic		Disabled
DHCP Client	Started	Automatic	Started	Automatic
Distributed File System	Started	Automatic		Disabled
Distributed Link Tracking Client	Started	Automatic	Started	Automatic
Distributed Link Tracking Server		Manual		Disabled
Distributed Transaction Coordinator	Started	Automatic		Disabled
DNS Client	Started	Automatic	Started	Automatic
Event Log	Started	Automatic	Started	Automatic
Fax Service		Manual		Disabled
File Replication		Manual		Disabled
Indexing Service		Manual		Disabled
Internet Connection Sharing		Manual		Disabled
Intersite Messaging		Disabled		Disabled
IPSEC Policy Agent	Started	Automatic		Disabled
Kerberos Key Distribution Center		Disabled		Disabled
License Logging Service	Started	Automatic		Disabled
Logical Disk Manager	Started	Automatic	Started	Automatic
Logical Disk Manager Administrative Service		Manual		Manual
Messenger	Started	Automatic		Disabled
Net Logon	Started	Automatic	Started	Automatic
NetMeeting Remote Desktop Sharing		Manual		Disabled
Network Associates Alert Manager	Started	Automatic	Started	Not Defined
Network Associates McShield	Started	Automatic	Started	Not Defined
Network Associates Task Manager	Started	Automatic	Started	Not Defined
Network Connections	Started	Manual	Started	Manual
Network DDE		Manual		Disabled
Network DDE DSDM		Manual		Disabled
NT LM Security Support Provider		Manual		Disabled
Performance Logs and Alerts		Manual		Manual
Plug and Play	Started	Automatic	Started	Automatic
Print Spooler	Started	Automatic	Started	Automatic
Protected Storage	Started	Automatic	Started	Automatic
QoS RSVP		Manual		Disabled
Remote Access Auto Connection Manager		Manual		Disabled

	Default Computer Setting		MS Baseline Policy	
	Status	Startup Type	Status	Startup Type
Remote Access Connection Manager		Manual		Disabled
Remote Procedure Call (RPC)	Started	Automatic	Started	Automatic
Remote Procedure Call (RPC) Locator		Manual		Disabled
Remote Registry Service	Started	Automatic	Started	Automatic
Removable Storage	Started	Automatic		Disabled
Routing and Remote Access		Disabled		Disabled
RunAs Service	Started	Automatic		Disabled
Security Accounts Manager	Started	Automatic	Started	Automatic
Server	Started	Automatic	Started	Automatic
Smart Card		Manual		Disabled
Smart Card Helper		Manual		Disabled
System Event Notification	Started	Automatic	Started	Automatic
Task Scheduler	Started	Automatic		Disabled
TCP/IP NetBIOS Helper Service	Started	Automatic	Started	Automatic
Telephony	Started	Manual		Disabled
Telnet		Manual		Disabled
Terminal Services	Started	Automatic		Disabled
Uninterruptible Power Supply		Manual		Disabled
Utility Manager		Manual		Disabled
VMware Tools Service	Started	Automatic	Started	Not Defined
Windows Installer		Manual		Disabled
Windows Management Instrumentation	Started	Automatic		Disabled
Windows Management Instrumentation Driver Extensions	Started	Manual	Started	Manual
Windows Time	Started	Automatic	Started	Automatic
Workstation	Started	Automatic	Started	Automatic

One of the most common security Best Practices is to disable services that are not needed as these can be misused by launching an attack on that service, such as exploiting a buffer-overflow vulnerability, and disrupting normal operation of the computer. These services also often run in the context of the LocalSystem account which has access to everything on the computer so that hijacking that service could allow an attacker to access other parts of the server or run their own program in the context of the LocalSystem account. While Microsoft disables or disables the startup of a number of services installed by default, fewer services are absolutely needed for a server to run. Disabling services, however, can disrupt desired functionality such as creating Performance Monitor alerts on the server or being able to schedule scripts to run at specified times. In general, though, the fewer unnecessary services, the better. In addition to the services in bold type, the Baseline template also specifies other services as well which are not installed as part of a standard Windows 2000 member server installation. [8] (Microsoft Security Operations Guide pp.64-65, Appendix C: Additional Services) The template also tightens the permissions on these services to restrict full access to the local

Administrators group and System account and provide only the Interactive user with read access, instead of granting read access to the Authenticated users group as a default installation does.

Additional Security Options

The Microsoft Baseline security policy also alters Registry values for the following:

MACHINE\System\CurrentControlSet\Control\LSA\NoLMHash=4,1

This setting ensures that LanManager hashes, which can easily be cracked, are not stored in the SAM database on the machine. For a file server, these would be the LM hashes for the passwords of local accounts. Changing this setting, however, only effects accounts created from that point on or when passwords are next changed. Even though a file server would typically not have extra local accounts, this can help protect the Administrator account password as long as this password is changed after this policy is applied.

MACHINE\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation=4,1

There are exploits that make use of the 8.3 DOS files names generated for backward compatibility if two files with different NTFS permissions in different directories end up having the same 8.3 name. This value turns off the generation of these names, although again from the point that it is changed. To delete these 8.3 names, the files need to be copied from the server, deleted on the server and copied back to the server.

MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog=4,20000
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog=4,20
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\DynamicBacklogGrowthDelta=4,10
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxPortsExhausted=4,5
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions=4,3
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions=4,2
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=4,2
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=4,300000
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=4,2
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableSecurityFilters=4,1
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=4,0

These keys modify a number of settings related to the TCP/IP network stack and the Afd.sys driver to help prevent denial of service as a result of SYN flooding attacks on a server. This can be the result of attacks where large numbers of network connections are made that do not complete the three-way protocol handshake. This type of attack is designed to consume enough system resources that the server becomes unavailable to further network connections.

File System Permission Changes

	Default Installation	MS Baseline
%systemdrive%\	Everyone: Full Control	Administrators: Full control System: Full control

		Authenticated Users: Read and Execute, List Folder Contents, Read
%SystemRoot%\Repair %SystemRoot%\Security %SystemRoot%\Temp %SystemRoot%\system32\Config %SystemRoot%\system32\Logfiles	Administrators: Full control Creator/Owner: Full Control System: Full control Power Users: * Users: **	Administrators: Full control Creator/Owner: Full Control System: Full control
%systemdrive%\inetpub	Everyone: Full Control	Administrators: Full control System: Full control Everyone: Read and Execute, List Folder Contents, Read
* Power Users - Repair: Modify, Security: Read & Exec, Config: Read & Exec, LogFiles: Modify ** Users - Repair: Read & Exec, Security: Read & Exec, Config: Read & Exec, LogFiles: Read & Exec		
Based on Table 4.11: Settings to Secure Key Directories Defined in the Member Server Baseline Policy, Microsoft Security Operations Guide, 2002, p. 63		

The Microsoft Baseline security template adjusts the NTFS permissions on a number of system directories from that of a standard Windows 2000 Server installation. The most important of these is to that of the default permissions on the system drive, which in turn are automatically inherited to subfolders that use Inheritance and are used on newly created directories. By default, the Everyone group has Full Control. While one would typically restrict access to shared directories via NTFS or share permissions, this default makes it easy to give people too much access to data on a server in place of too little. The template's setting, however, only adjusts the default permissions on the system drive and does not affect other drives, which is where shared data would typically be stored on a file server.

Furthermore, the Baseline security template tightens the NTFS permissions on several system32 subdirectories. This is primarily to restrict access to these directories to members of the Administrators group, and when needed, to provide restricted access to the Users group. The template also tightens permissions on the World Wide Web server directory, Inetpub, where the default WWW root is often located to give the Everyone group Read & Execute, List and Directory Traversal privileges instead of Full Control. While one should further restrict these permissions on a web servers directories to the absolute minimum required, this default is better than the Full Control default permission which is set at the time a server is installed. Finally the Baseline template also restricts access to a number of system files to only the Administrators group, as indicated in Appendix A: Additional Files Secured in the Microsoft Operation Security Guide.

Registry Permissions Changes

While the Microsoft Baseline security template contains a number of Registry permission entries, a comparison of these with the default registry permissions applied during installation of Windows 2000 server showed only two differences between the two.

"MACHINE\Software",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"MACHINE\Software\Classes",2,"D:(A;CI;GR;;;WD)"

The primary effect of the Registry permissions in the Baseline policy is to restrict the Power Users group to Read level access to the Local_Machine\Software and Locak_Macine\Software\Classes keys and any sub-keys that inherit their permissions. With a default installation members of the Power Users group have modify and delete privileges on these keys. This was done to provide greater backward compatibility with the Windows NT local groups structure but the Baseline template restricts modification of these keys to Administrators and the System account to minimize the number of users that could modify these keys given their importance to the proper function of software installed on the computer.

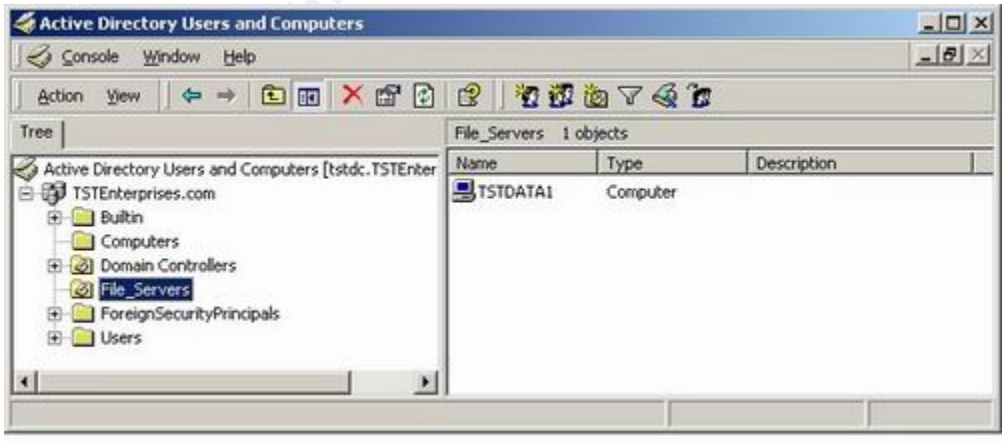
Restricted Groups

Restricted Groups allows users to be specified that are authorized to be members of a particular group such as Administrators. If another user is added to the group and is not on the list of users in the group in the Restricted Groups policy, then that account will be removed from the group when the policy is applied. The Microsoft Baseline security template does not specify any Restricted Groups settings.

Application of Template

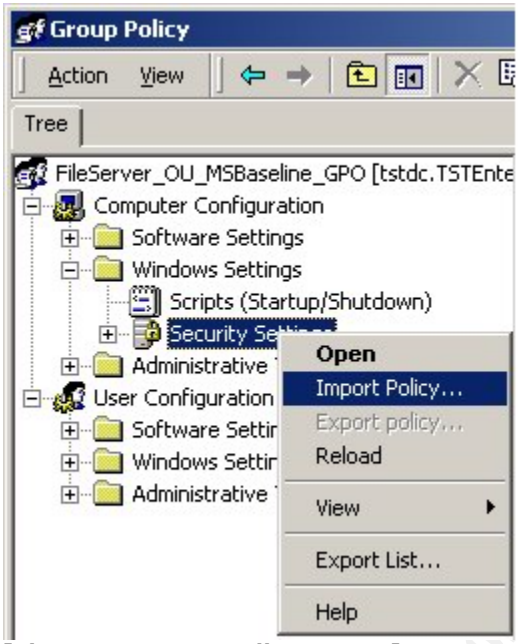
The Microsoft Baseline security template was tested in a single domain Windows 2000 environment with one domain controller, two member servers and one Windows 2000 Professional workstation. This domain uses Active Directory in native mode.

The template was distributed using two AD Group Policy policies assigned to a File_Servers Organizational Unit for file servers. The TSTDATA1 server was added to this OU while the TSTDATA2 was left in the Computers OU to be able to compare the two servers after the template was distributed.

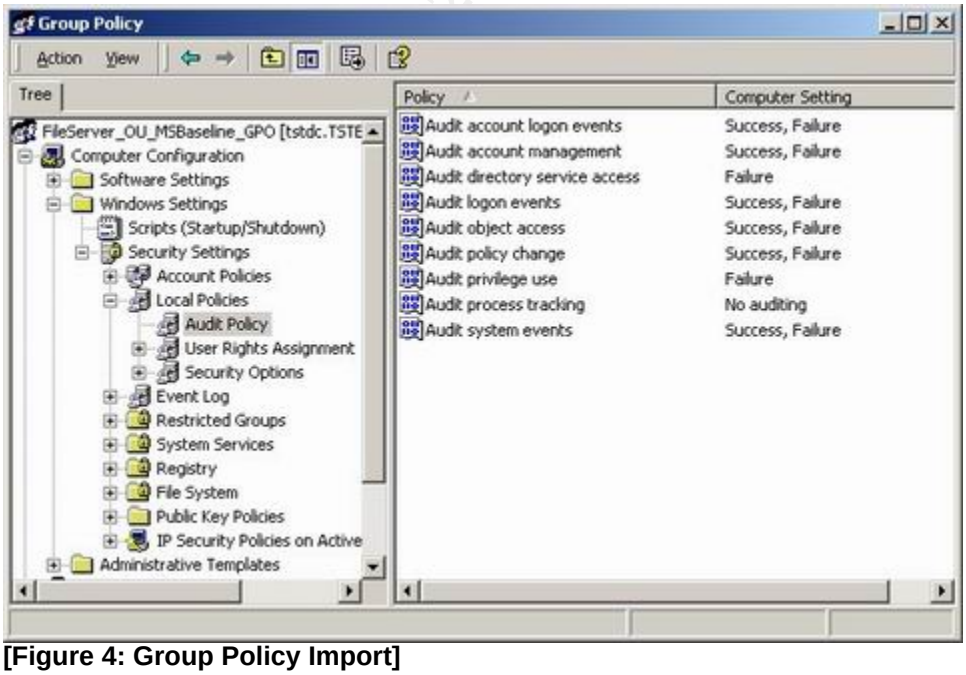


[Figure 2: Active Directory structure]

In the Active Directory Users and Computers console, an Organizational Unit was created titled File_Servers. Then a Group Policy object was created using the Group Policy item on the Properties for that Organizational Unit. After creating the Group Policy object, a console to modify it was opened using the Edit button on the Group Policy window. In this console, the Microsoft Baseline template was then imported using Import Policy menu item on the Computer Configuration / Windows Settings / Security Settings Group Policy item.

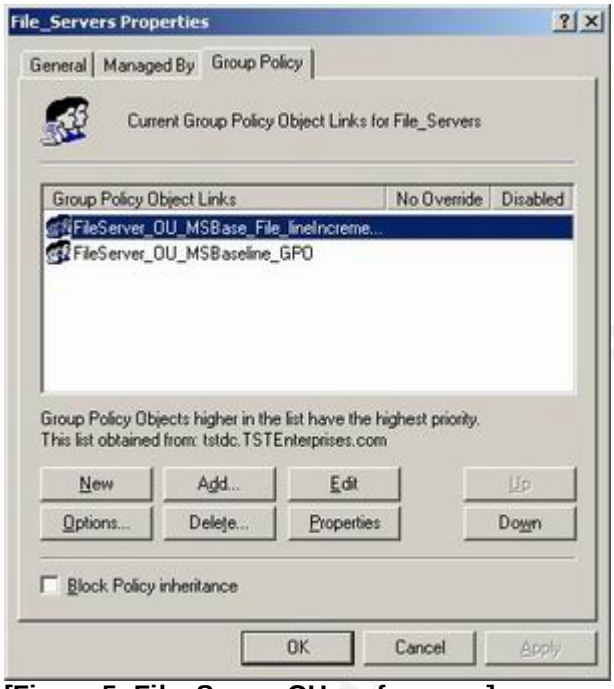


[Figure 3: Group Policy Import]



[Figure 4: Group Policy Import]

Because the Microsoft Baseline template comes in two templates, one for various server types and incremental templates for specific server roles, a second Group Policy policy was created for the File and Print Incremental template. This policy was then edited and the template was imported as was done with the first policy. Because there were now two policies assigned to the File_Server Organizational Unit, the Group policy with the settings from the File and Print Incremental template was moved to the first position in the list of policies to ensure that it would be processed after the first policy with the Baseline template settings to ensure that its settings took precedence over the general settings. One of these disabled the Print Spooler service which would prevent users from being able to print the print queues on a server with this Group policy.



[Figure 5: File_Server OU preferences]

The policies on the TSTDATA1 server were then manually refreshed using the following commanding a DOS window:

secedit /refreshpolicy machine_policy

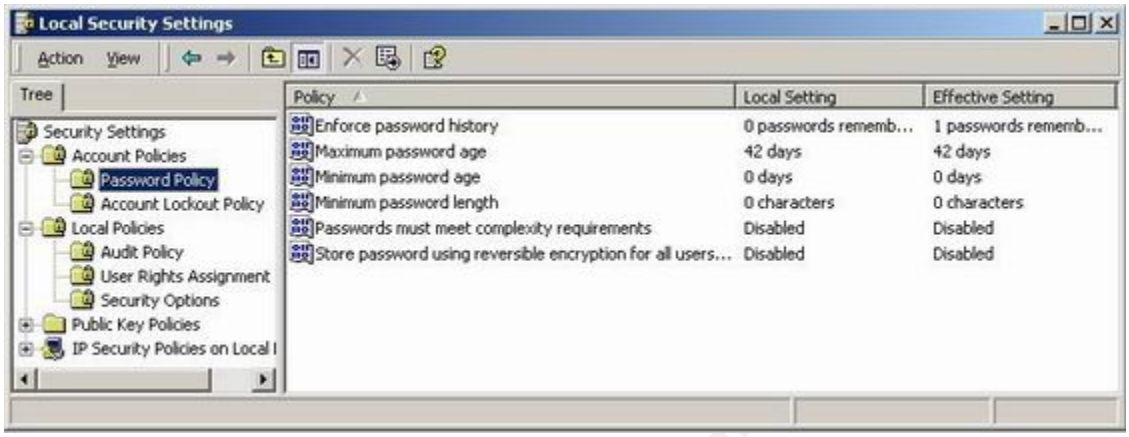
Testing of Template

Test of security settings

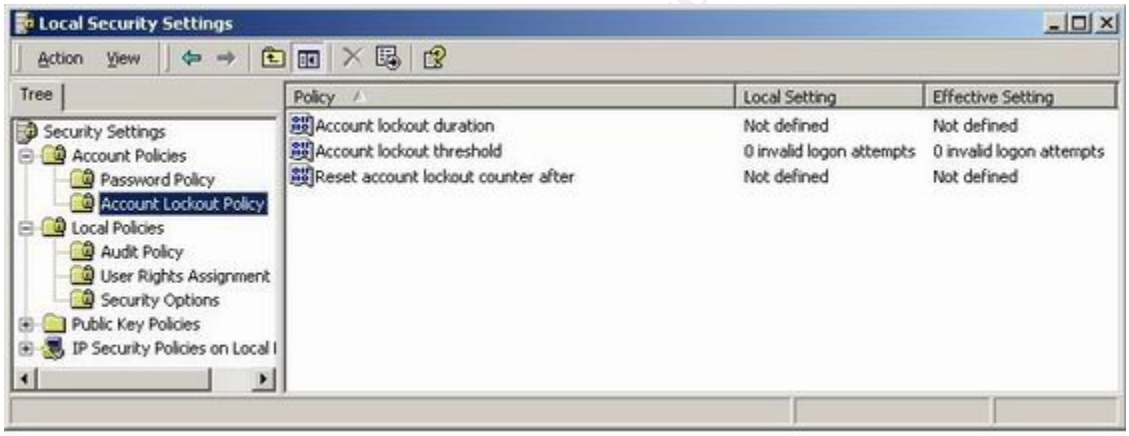
1. Analysis of system policies in effect on TSTDATA1 server

The application of the security settings were confirmed using the Local Security Settings console on the TSTDATA1 server. In this console, the settings in the Local Setting are those defined in the local system policy and those in the Effective Setting column are those applied from the Group Policy policies, which include both the Default Domain policy and the two Group policies assigned to the

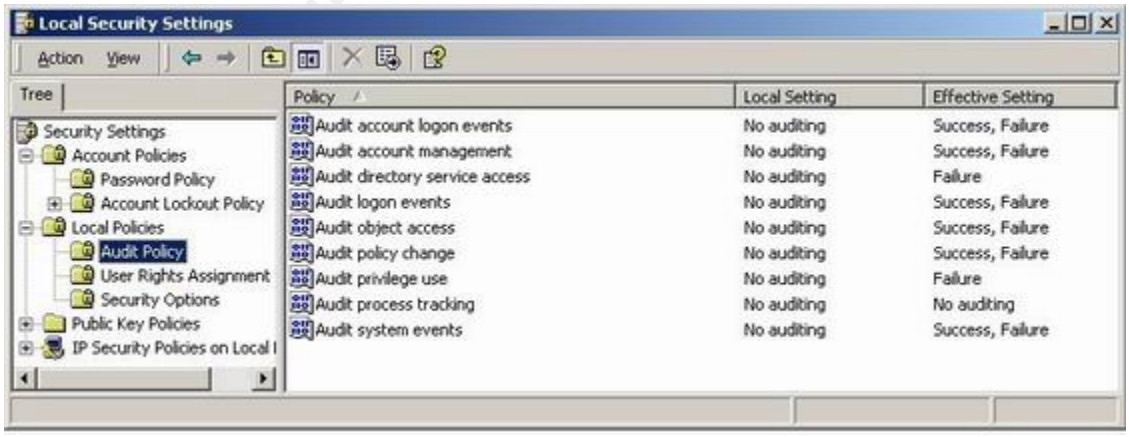
File_Server Organizational Unit. There are no other Group Policy objects assigned to the site or domain. From the following screenshots, we can see which settings are in effect on the TSTDATA1 file server which is a member of the File_Servers Organizational Unit in the TSTEnterprises domain.



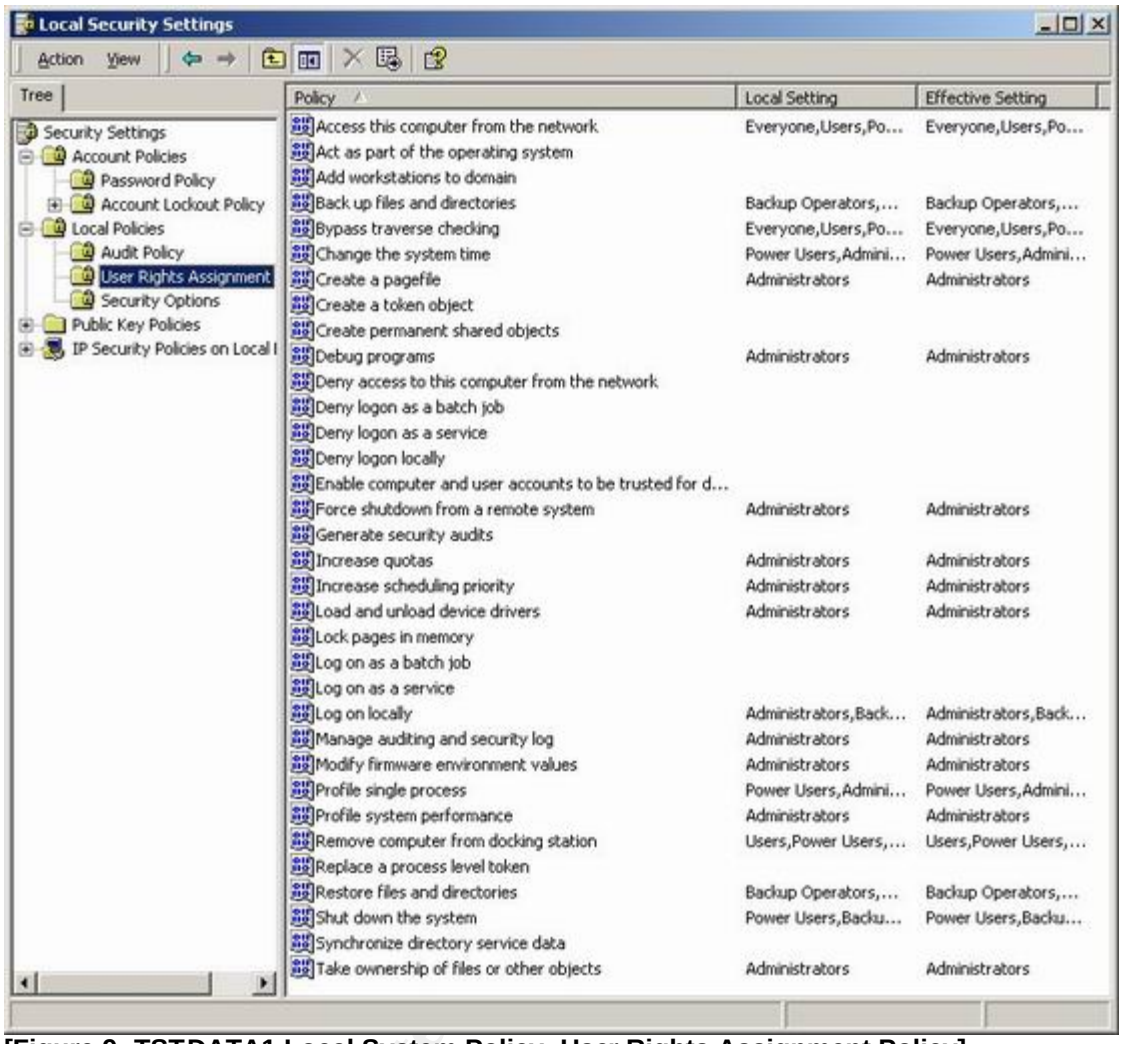
[Figure 6: TSTDATA1 Local System Policy: Password Policy]



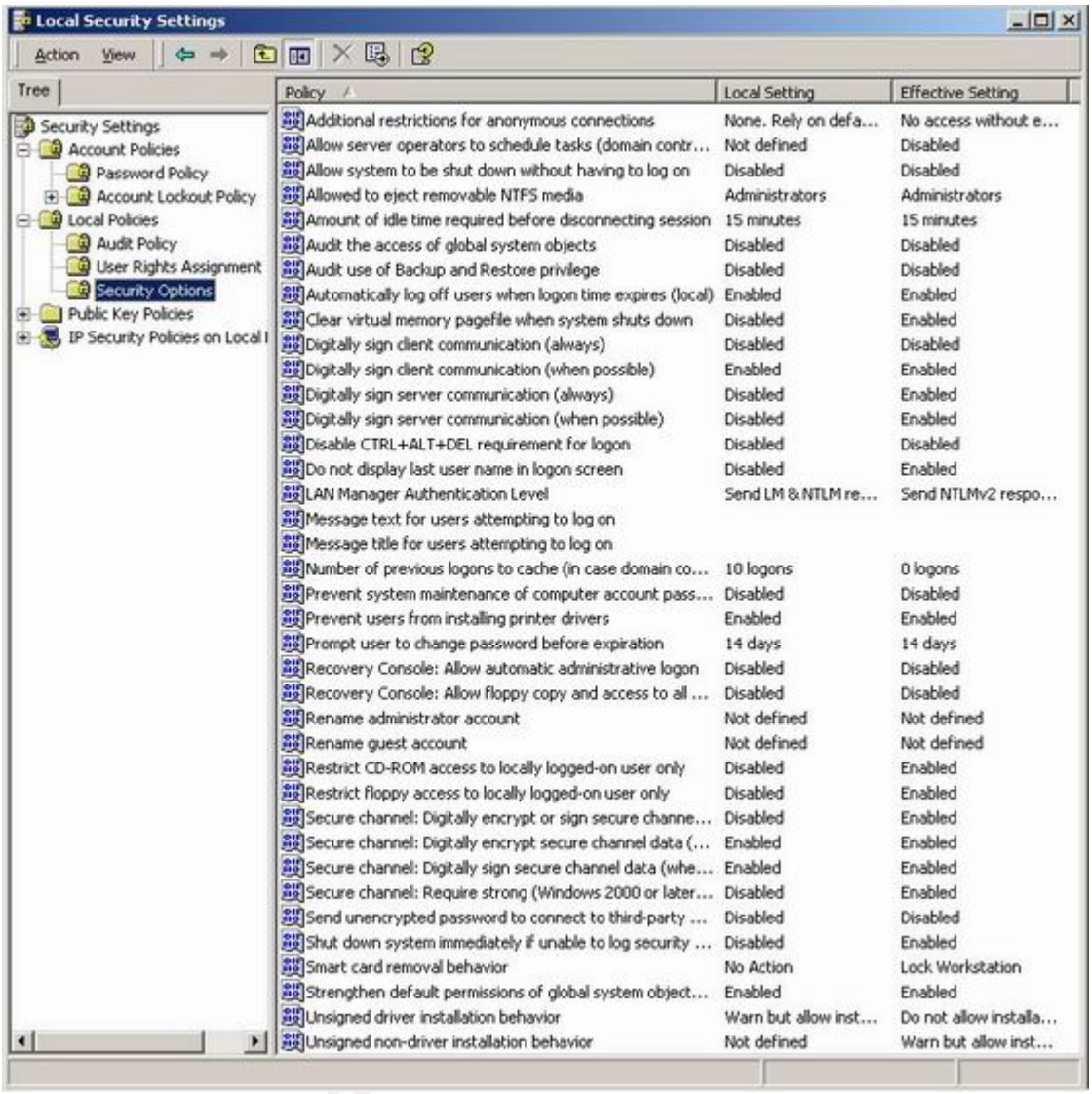
[Figure 7: TSTDATA1 Local System Policy: Account Lockout Policy]



[Figure 8: TSTDATA1 Local System Policy: Audit Policy]



[Figure 9: TSTDATA1 Local System Policy: User Rights Assignment Policy]



[Figure 10: TSTDATA1 Local System Policy: Security Options Policy]

A check of a selection of Local System policies on the TSTDATA2 server, which was not a member of the File_Server Organizational Unit for testing purposes, shows that these settings remained the same as the default configuration. Thus, the Group Policy policies were applied only to the intended servers

Figure 11: TSTDATA2 Local System Policy: Audit Policy]

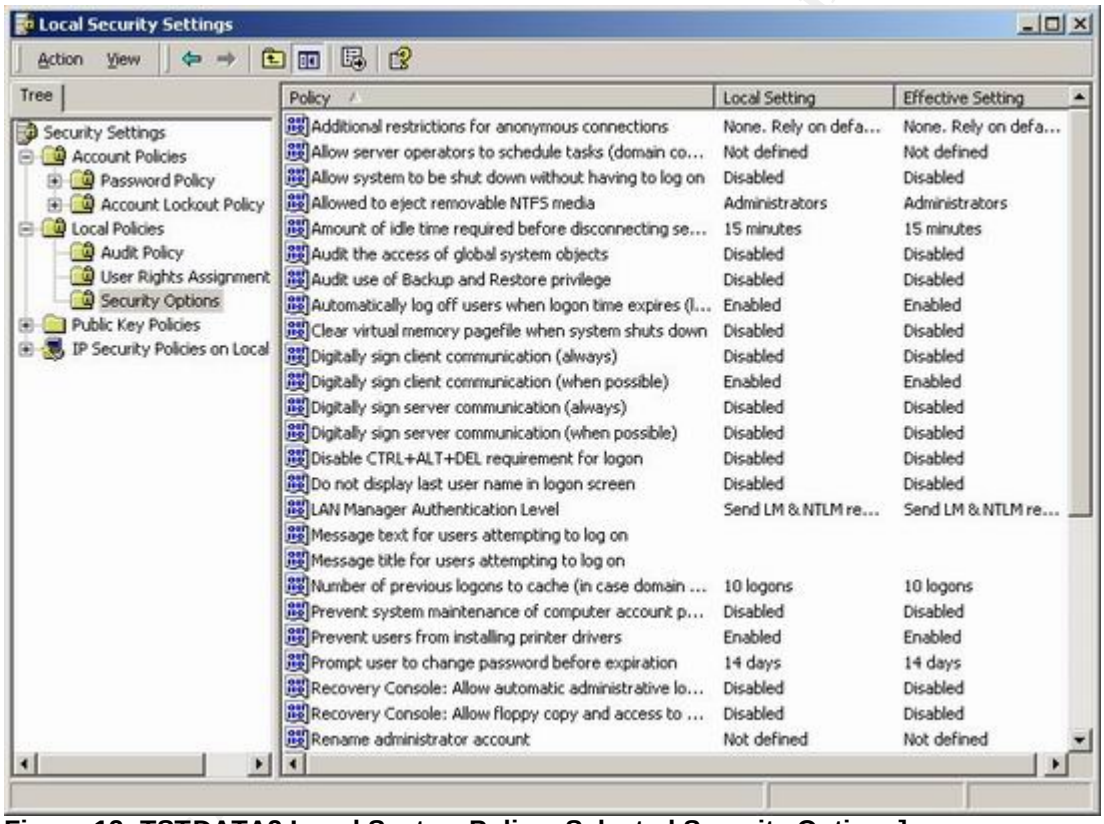


Figure 12: TSTDATA2 Local System Policy: Selected Security Options]

2. Status of System Services

The Microsoft Baseline security template also specified a number of services which would be disabled to prevent attacks on unnecessary services. A check of the services on TSTDATA1 showed the following servers were disabled. The last column shows the startup type for the service as it is defined with a default installation of Windows 2000 Server. The primary effect of the policy is to disable a number of unnecessary services, which indeed occurred.

The Terminal Services service is also disabled in the Baseline template rendering a server unreachable via a Terminal Services Client session for remote administration. To correct this, the service must be enabled in the Group Policy File_Server_OU_MSBase_Incremental policy for the File_Servers Organizational Unit.

Name	Status	Startup Type	Log On As	Startup (Default Install)
Alerter		Disabled	LocalSystem	Automatic
Application Management		Disabled	LocalSystem	Manual
ClipBook		Disabled	LocalSystem	Manual
Computer Browser		Disabled	LocalSystem	Automatic
Distributed File System		Disabled	LocalSystem	Automatic
Distributed Link Tracking Server		Disabled	LocalSystem	Manual
Distributed Transaction Coordinator		Disabled	LocalSystem	Automatic
Fax Service		Disabled	LocalSystem	Manual
File Replication		Disabled	LocalSystem	Manual
Indexing Service		Disabled	LocalSystem	Manual
Internet Connection Sharing		Disabled	LocalSystem	Manual
Intersite Messaging		Disabled	LocalSystem	Disabled
IPSEC Policy Agent		Disabled	LocalSystem	Automatic
Kerberos Key Distribution Center		Disabled	LocalSystem	Disabled
License Logging Service		Disabled	LocalSystem	Automatic
Messenger		Disabled	LocalSystem	Automatic
NetMeeting Remote Desktop Sharing		Disabled	LocalSystem	Manual
Network DDE		Disabled	LocalSystem	Manual
Network DDE DSDM		Disabled	LocalSystem	Manual
NT LM Security Support Provider		Disabled	LocalSystem	Manual
QoS RSVP		Disabled	LocalSystem	Manual
Remote Access Auto Connection Manager		Disabled	LocalSystem	Manual
Remote Access Connection Manager		Disabled	LocalSystem	Manual
Remote Procedure Call (RPC) Locator		Disabled	LocalSystem	Manual
Removable Storage		Disabled	LocalSystem	Automatic
Routing and Remote Access		Disabled	LocalSystem	Disabled
RunAs Service		Disabled	LocalSystem	Automatic
Smart Card		Disabled	LocalSystem	Manual
Smart Card Helper		Disabled	LocalSystem	Manual
Task Scheduler		Disabled	LocalSystem	Automatic
Telephony		Disabled	LocalSystem	Manual
Telnet		Disabled	LocalSystem	Manual
Terminal Services		Disabled	LocalSystem	Automatic
Uninterruptible Power Supply		Disabled	LocalSystem	Manual
Utility Manager		Disabled	LocalSystem	Manual
Windows Installer		Disabled	LocalSystem	Manual
Windows Management Instrumentation		Disabled	LocalSystem	Automatic

Figure 13: TSTDATA1 Disabled services]

To ensure that the Group Policy police based on the Baseline security template was only applied to the File_Server OU, the status of a selection of services that would have been disabled by the policy were also checked on theTSTDATA2 server. These were started automatically as they should have been since this

server is not a member of the Fiel_Servers OU and did not hence receive the File_Server OU Group policies.

Name	Status	Startup Type	Log On As	Startup (Default Install)
Alerter	Started	Automatic	LocalSystem	Automatic
Computer Browser	Started	Automatic	LocalSystem	Automatic
Distributed File System	Started	Automatic	LocalSystem	Automatic
Distributed Transaction Coordinator	Started	Automatic	LocalSystem	Automatic
IPSEC Policy Agent	Started	Automatic	LocalSystem	Automatic
License Logging Service	Started	Automatic	LocalSystem	Automatic
Messenger	Started	Automatic	LocalSystem	Automatic
Removable Storage	Started	Automatic	LocalSystem	Automatic
RunAs Service	Started	Automatic	LocalSystem	Automatic
Task Scheduler	Started	Automatic	LocalSystem	Automatic
Terminal Services	Started	Automatic	LocalSystem	Automatic
Windows Management Instrumentation	Started	Automatic	LocalSystem	Automatic

Figure 14: TSTDATA2 Status of Selected System Services]

3. Test of system behavior affected by template settings

The effect of several security settings can be directly observed on the system after the Group Policy has been applied.

The logon screen no longer displays the name of the last person to have logged in locally on the computer.

Figure 15: TSTDATA1 logon screen]

The Security log properties have been changed to increase the maximum size and to specify that the log must be cleared manually.

Figure 16: TSTDATA1 Security log settings]

Autorun programs are no longer automatically started when inserting a CD-ROM that normally runs a setup program from the CD-ROM.

Another security setting enabled from the Microsoft Baseline security template governs a restriction on the installation of unsigned driver and non-driver software. Digitally signing software, especially drivers, helps to ensure the authenticity of the software being installed as some hacking incidents have taken advantage of modifying trusted driver software to include a backdoor Trojan horse program or virus.

Not all driver software, however, is digitally signed and when trying to install a printer driver on the TSTDATA1 server, I received the following alert dialog box. The alert is missing the Yes button to allow the driver to be installed even though it is not digitally signed. This is because the File_Servers OU policy with the settings from the Baseline security template has set the “Unsigned driver installation behavior” security option to “Do not allow installation”.

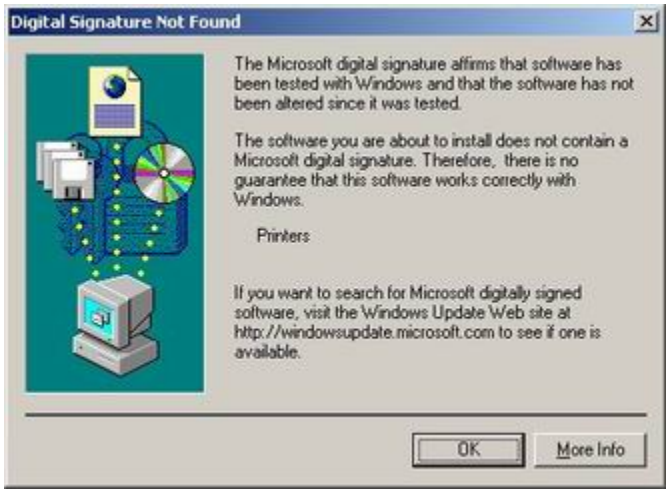


Figure 17: TSTDATA1 Unsigned Driver Alert]

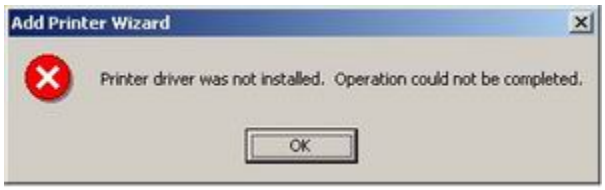


Figure 18: TSTDATA1 Printer driver installation failure]

To change this behavior, the Group Policy File_Server OU policy must be changed to at least a value of "Warn but allow installation" for this option. Changing this setting in the local system policy of the machine is not enough since the Organizational Unit policy is processed after local policies and takes thus precedence over local policies. Since not all print drivers are distributed digitally signed, this can be a troublesome setting for a print server but I will comment more on this when evaluating the security template.

4. Scan of server using a null session account

One of the most significant changes that the Microsoft Baseline template makes is that of restricting anonymous access to a computer. This access comes from null sessions created for connections from local or domain accounts that are not authorized to access the computer, such as having the "Access this computer from the network" user right. This is used by some applications and computers from trusted domains. With a default Windows 2000 operating system installation, information such as the local accounts, groups and shares could be read out by someone without an account on that server. This information can then be used by someone to map the resources on a network to further target hacking attempts.

The most secure setting, "No Access without Explicit Anonymous Access"- which the Baseline template uses, could case problems with applications requiring null session access. Null access to registry keys can be adjusted by adding paths to Registry keys in the following Registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPaths

Null session shares or named pipes can be defined by adding share or pipe names to the corresponding Registry key:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionShares
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionPipes

To test the result of the "Additional restrictions for Anonymous connections", the TSTDATA1 and TSTDATA2 servers were scanned with a null session scanning tool, GNIT which is available online from SecurityFocus at http://online.securityfocus.com/tools/1286. The TSTDATA1 sever had the Microsoft Baseline template applied to it via Group Policy and the TSTDATA2 did not. The GNIT tool was run while logged on with a local account on the TSTDesktop123 workstation which did not have any privileges on either of the file server computers.

```
GNIT Scanner . Ellicit Edition . by glitch

============================================================
Scan Results for 194.10.10.22
============================================================

------------------------------------------------------------
NBTSTAT Results from 194.10.10.22:
------------------------------------------------------------

Local Area Connection:
Node IpAddress: [194.10.10.25] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status

    ---------------------------------------------

    TSTDATA1      <00>  UNIQUE
    TSTENTERPRISES <00>  GROUP
    TSTDATA1      <20>  UNIQUE
    TSTDATA1      <03>  UNIQUE
    TSTENTERPRISES <1E>  GROUP

    MAC Address = 00-50-56-42-80-47

------------------------------------------------------------
NetView Results from 194.10.10.22
------------------------------------------------------------
Could not Net View Target or No Entries to show

------------------------------------------------------------
Groups and Users Present On Server:
------------------------------------------------------------

------------------------------------------------------------
```

```
Attempting to enumerate tranports avialable:
-------------------------------------------------------
Unnable to scan transports

This exe file was created with the evaluation version of Perl2Exe.
For more information visit http://www.perl2exe.com
(The full version does not display this message with a 2 second delay.)
...
```

[Figure 19: Output from GNIT null session scan of TSTDATA1 server]

The TSTDATA2 server, on the other hand, which did not have the Baseline policy revealed much more information to a null session scan from the TSTDesktop123 workstation.

```
GNIT Scanner . Ellicit Edition . by glitch

=============================================================
Scan Results for 194.10.10.23
=============================================================

-------------------------------------------------------------
NBTSTAT Results from 194.10.10.23:
-------------------------------------------------------------

Local Area Connection:
Node IpAddress: [194.10.10.25] Scope Id: []


           NetBIOS Remote Machine Name Table

       Name               Type         Status

    ---------------------------------------------

    TSTDATA2       <00>  UNIQUE
    TSTENTERPRISES <00>  GROUP
    TSTDATA2       <20>  UNIQUE
    TSTDATA2       <03>  UNIQUE
    TSTENTERPRISES <1E>  GROUP

    MAC Address = 00-50-56-42-80-66

-------------------------------------------------------------
NetView Results from 194.10.10.23
-------------------------------------------------------------
Shared resources at \\194.10.10.23

Share name   Type         Used as  Comment

-------------------------------------------------------------------------------
APPS1        Disk
DATA1        Disk
The command completed successfully.
```

```
-------------------------------------------------------------
Groups and Users Present On Server:
-------------------------------------------------------------

The groups are:
      Administrators
      Backup Operators
      Guests
      Power Users
      Replicator
      Users
      APPS_Users
      DATA_Users
      None

The list of user accounts are:
      Administrator
      Guest
      TsInternetUser

--------Details for Administrator:

Global Group Membership:
      None

Local Group Membership:
      Administrators

Account Expires: Never
Full Name:
Bad Password Attempts: 0
Comments: Built-in account for administering the computer/domain
Last Logon: Mon Jan 13 12:09:24 2003
Last Logoff: Thu Jan  1 01:00:00 1970
Logon Server: \\*
Successful Logins: 11
Password Age: Sat Jan 10 06:22:53 1970
Primary Group ID: 513
Privelege: Admin
RID: 500

--------Details for Guest:

Global Group Membership:
      None

Local Group Membership:
      Guests

Account Expires: Never
Full Name:
Bad Password Attempts: 0
Comments: Built-in account for guest access to the computer/domain
Last Logon: Thu Jan  1 01:00:00 1970
Last Logoff: Thu Jan  1 01:00:00 1970
Logon Server: \\*
Successful Logins: 0
```

```
Password Age: Thu Jan  8 09:14:59 1970
Primary Group ID: 513
Privelege: Guest
RID: 501

--------Details for TsInternetUser:

Global Group Membership:
      None

Local Group Membership:
      Guests

Account Expires: Never
Full Name: TsInternetUser
Bad Password Attempts: 0
Comments: This user account is used by Terminal Services.
Last Logon: Thu Jan  1 01:00:00 1970
Last Logoff: Thu Jan  1 01:00:00 1970
Logon Server: \\*
Successful Logins: 0
Password Age: Fri Jan  9 22:28:33 1970
Primary Group ID: 513
Privelege: Guest
RID: 1000

------------------------------------------------------------
Attempting to enumerate tranports avialable:
------------------------------------------------------------
\Device\NetbiosSmb
\Device\NetBT_Tcpip_{F426FF29-4CC7-421B-A100-C27999708C4D}

This exe file was created with the evaluation version of Perl2Exe.
For more information visit http://www.perl2exe.com
(The full version does not display this message with a 2 second delay.)
...
```

[Figure 20: Output from GNIT null session scan of TSTDATA2 server]

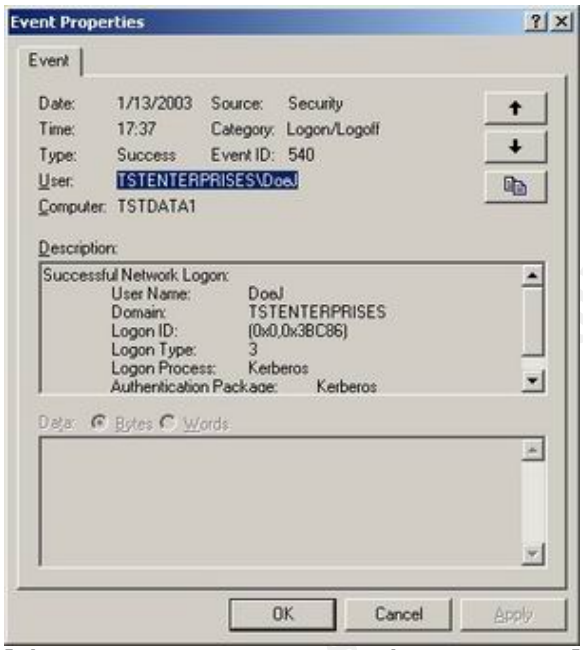
Conducting this scan with the GNIT tool, however, from a regular domain account which did not have any authorization on the TSTDATA1 server, also revealed the as much information as a scan of the TSTDATA2 server. This is because the "Additional restrictions for anonymous connections" does not place additional restrictions on authenticated user accounts. This makes it possible for one to use a regular domain or local account for reconnaissance purposes.

5. Security log events

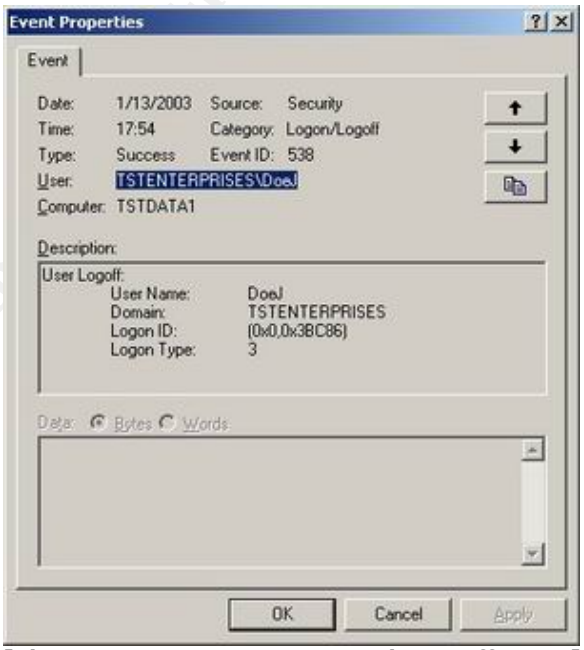
The enabling of security-related Auditing is also one of the important tasks of improving the security of a Windows server. This is because these logged events help to identify what, when and by whom something has occurred on a system. For the purposes of the TSTDATA1 file server, the impact of the Microsoft Baseline security template can be seen by the Security log events generated by accessing of a share on that server from the TSTDesktop123 workstation via the network.

Security Event Log: when a share on TSTDATA1 is accessed

Success Audit	1/13/2003	5:37:32 PM	Security	Logon/Logoff	540	DoeJ	TSTDATA1
Success Audit	1/13/2003	5:37:35 PM	Security	Logon/Logoff	540	TSTDESKTOP123$	TSTDATA1
Success Audit	1/13/2003	5:40:08 PM	Security	Logon/Logoff	538	TSTDESKTOP123$	TSTDATA1
Success Audit	1/13/2003	5:54:10 PM	Security	Logon/Logoff	538	DoeJ	TSTDATA1



[Figure 21: TSTDATA1 Network Logon event]



[Figure 22: TSTDATA1 Network Logoff event]

Furthermore, network logon failures are also logged such as these events which were generated when scanning the TSTDATA1 server with the GNIT tool while logged on with a local account on the TSTDesktop123 workstation to test a null session. While workstation name is provided with these logon failures from Windows NT and higher clients, workstation names of Windows 9x clients are not provided, making it more difficult to pinpoint logon failures from these computers.

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 1/13/2003
Time: 5:32:23 PM
User: NT AUTHORITY\SYSTEM
Computer: TSTDATA1

Description:
The logon to account: ParkJ
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: TSTDESKTOP123
failed. The error code was: 3221225572

Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 1/13/2003
Time: 5:32:23 PM
User: NT AUTHORITY\SYSTEM
Computer: TSTDATA1
Description:
Logon Failure:
Reason: Unknown user name or bad password
User Name: ParkJ
Domain: TSTDESKTOP123
Logon Type: 3
Logon Process: NtLmSsp
Authentication Package: NTLM
Workstation Name: TSTDESKTOP123

Since the security settings are applied via Group Policy, one can see when the policy is applied to a machine, such as when it is booted, in the following security log event from the TSTDATA1 server.

Event Type: Success Audit
Event Source: Security
Event Category: Policy Change
Event ID: 612
Date: 1/14/2003
Time: 9:27:19 AM
User: NT AUTHORITY\SYSTEM
Computer: TSTDATA1
Description:
Audit Policy Change:
New Policy:

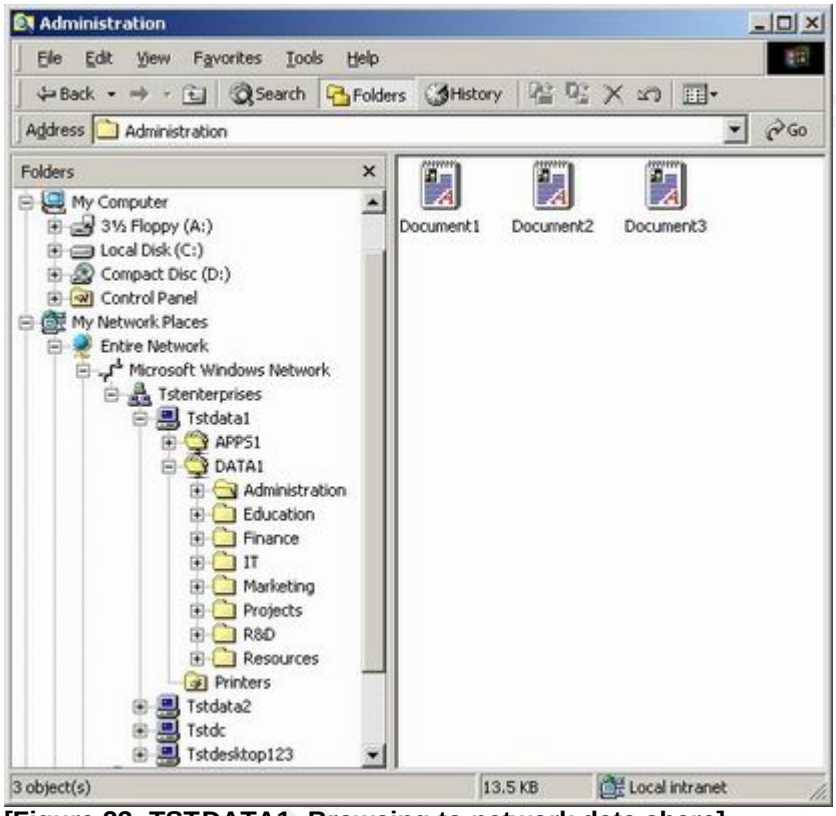
Success		Failure
+	+	Logon/Logoff
+	+	Object Access
-	+	Privilege Use
+	+	Account Management
+	+	Policy Change
+	+	System
-	-	Detailed Tracking
-	+	Directory Service Access
+	+	Account Logon

Changed By:
User Name: TSTDATA1$
Domain Name: TSTENTERPRISES
Logon ID: (0x0,0x3E7)

Functional test of system

1. Browse to a file on share

The primary function of a file server is to provide a central data store where users can share documents or applications with each other. This was tested by logging into the TDTDestop123 workstation with a domain account which had access to the data shares on the TSTDATA1 file server, browsing to that server with Network Neighborhood and opening a document in the Administration directory on the DATA1 share.

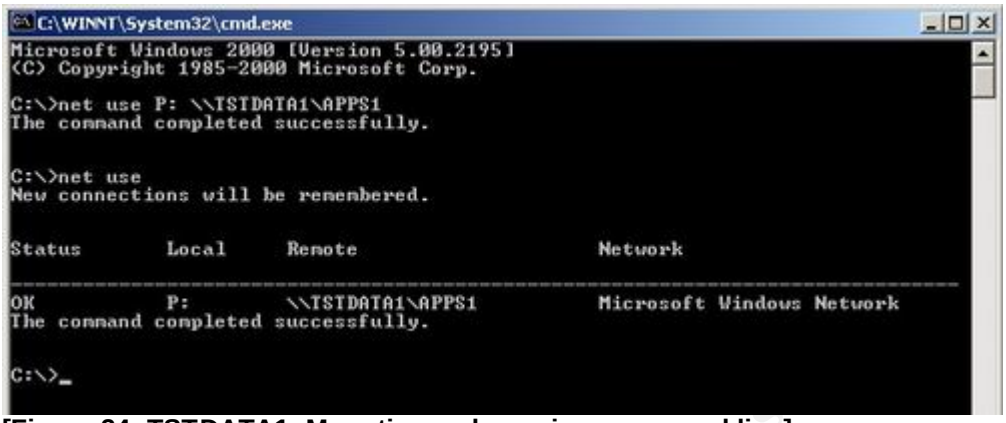


[Figure 23: TSTDATA1: Browsing to network data share]

This was successful and generated the following Security log events.

Success Audit	1/13/2003	5:37:32 PM	Security	Logon/Logoff	540	DoeJ	TSTDATA1
Success Audit	1/13/2003	5:37:35 PM	Security	Logon/Logoff	540	TSTDESKTOP123$	TSTDATA1
Success Audit	1/13/2003	5:40:08 PM	Security	Logon/Logoff	538	TSTDESKTOP123$	TSTDATA1
Success Audit	1/13/2003	5:54:10 PM	Security	Logon/Logoff	538	DoeJ	TSTDATA1

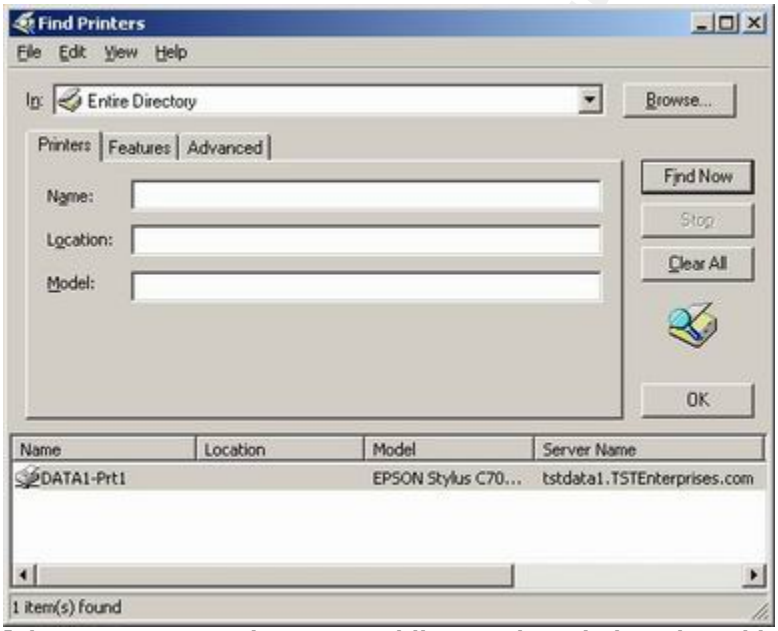
The APPS1 share was also mounted using a net use command from a DOS command prompt to test mounting a share from the command line such as in a logon script. This operation was also successful.



[Figure 24: TSTDATA1: Mounting a share via a command line]

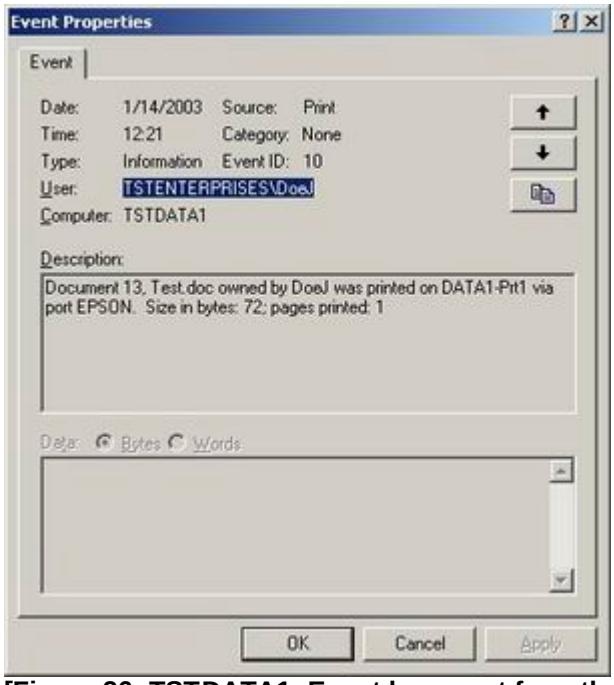
2. Add printer from server and print document

Since file servers are often used to also share printers, a printer being shared on the TSTDATA1 server was added by a domain user on the TSTDesktop123 workstation and a test document was printed.



[Figure 25: TSTDesktop123: Adding a printer being shared by TSTDATA1 server]

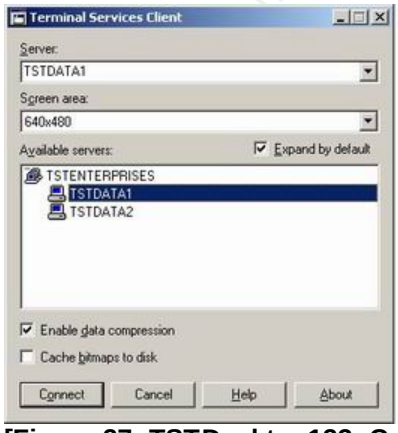
As the Event log entries confirm, the document printed successfully.



[Figure 26: TSTDATA1: Event log event from the printing of the test document]

3. Connect with Terminal Services Client to remote administer file server

Connecting to the TSTDATA1 server with Terminal Services Client from the TSTDATA1 workstation initially ran into a snag. The TSTDATA1 server was not available in the Terminal Services Client because the Terminal Services service was disabled as a result of the Microsoft Baseline template System Services settings. To resolve this, the startup of the Terminal Services service was changed to Automatic in the File_Servers Group Policy MS_Baseline policy and the policies on the TSTDATA1 server were refreshed with the secedit command. The server was then restarted to ensure that the service was started automatically by a boot of the server. This was indeed the case and a connection to the server could be made from Terminal Service Client on the TSTDestiop123 workstation.



[Figure 27: TSTDesktop123: Connecting to TSTDATA1 via Terminal Services Client]

[Figure 28: TSTDesktop123: Terminal Services session to remotely administer TSTDATA1]

Evaluation of Template

Appropriateness of template

Making a Windows 2000 server more secure involves a range of activities, both organizational and technical, to reduce the possibility that the server or its resources are misused. A security template can be used to configure a number of registry settings, file and registry permission and system services options. These settings, however, must balance providing adequate functionality and manageability of a system with efforts to make it more secure, given its role in a company's computing environment.

When configuring access control list permissions to a system's resources, one can either begin with very open access as a default and restrict that access as needed or, as if often recommended, begin with the most restrictive permissions that still grant the desired functionality and to relax those restrictions as needed. Similarly, some security templates specify settings for only a few critical security-related settings and leave the others unaffected while others configure a broad range of settings with stricter settings, sometimes at the expense of system functionality or flexibility. The Microsoft Baseline security template and File and Print Incremental template were selected for evaluation since they scored the highest on the amount of security added to a default installation of Windows 2000 server relative to the impact that the settings would have on server performance or maintenance.

Best practices such as those outlined in the Microsoft Security Operations Guide suggest steps such as stricter account/password requirements, auditing of events on a system, implementation of a number of options to improve a system's security and the disabling of unnecessary services on a system. [9] (Microsoft TechNet, Security Operations Guide for Windows 2000 Server) Each of the templates that were investigated had both strengths and weaknesses in addressing these recommendations. Of the templates which were investigated, the basicsv.inf, securews.inf and CIS-Win2K-Level-I-v1.1.7.inf would provide greater compatibility and require less effort to implement since fewer settings and services were changed from that of a default Windows 2000 server installation. The other three templates, hisecws.inf, baseline.inf and w2k_server.inf, enable more options and configure settings more stringently but impact a server's functionality more than the other templates.

The Baseline and File and Print Incremental security templates do not alter the password and account policies from the local and domain default settings. The Microsoft Security Operations Guide indicates that this is done intentionally since these policies vary too much per organization to include in a general template. Because this template is intended for file and print servers, and local accounts are typically not used to provide access to resources on these servers, one can argue that the default settings are acceptable. Since application servers, on the other hand, often not only use local account, but local accounts with Administrator privileges to run application services and for application administration, more stringent password and account policies should be implemented on these servers.

The Baseline templates do, however, implement a much more balanced auditing and event log configuration than the other templates. While various auditing is enabled in all but the basicsv.inf template, the Event log settings are either left unchanged or set such that a server would require more maintenance or resources. The CIS-Win2K-Level-I-v1.1.7.inf template does not change the default Event log settings which would likely not provide enough storage space for the number of events generated by the audit policy. The w2k_server.inf, on the other hand, implements a maximum size of 4 GB on each of the three logs which would require ensuring that the logs were stored on a sufficiently large enough hard drive to prevent it from being filled up as a result of logged events. The Baseline.inf template configures a reasonable balance in terms of log size but does specify that the log must be cleared manually and that the server automatically shuts down if unable to log security events or its maximum size is reached. Since File and Print servers have a very high expectation for availability, these settings could case a server to shut down and disrupt access to its resources if the Security log is not closely monitored and regularly cleared. In many company's it may be desirable to implement an automated monitoring of the security log for unusually high numbers of events than to automatically shut the server down. In either case, this setting does require more care and maintenance on servers for which it is implemented.

The six security templates also differ from each other in terms of the additional Security Options that were configured. While the Baseline.inf template contains enough extra Security Options items to place a higher necessity of a Windows 2000 environment or adequate configuration of legacy clients, it also implements many Best Practice recommendations while not overly taxing a system's functionality or manageability. This includes options for SMB signing, Secure Channel signing/encryption, clearing of memory page files and cached logon credentials, restrictions on anonymous connections, NTLMv2 authentication, not storing LanManager hashes in the local SAM database, restricting network access to the floppy and CD-ROM drives and not displaying the last user to have logged on. Even though each of these items individually can pose a small risk of being exploited, the Baseline.inf covers the most bases without enabling the most or most stringent configuration for every possible setting. Of these settings, the requirement of digitally signing SMB communications and the use of NTMLv2 authentication could cause problems with older Windows clients such as 9x or NT desktops but these settings caused no problems in the tests of the template ion the TSTDATA1 file server.

The setting for the "Additional restrictions for anonymous connections" could also cause compatibility problems with some applications but did not cause any errors during the testing of the TSTDATA1 file server. If needed, this could be relaxed to a value of "Do not allow enumeration of SAM accounts and shares" for greater compatibility. Also, one should remember that this setting only restricts unauthenticated sessions from reading this information. Regular domain or local accounts could still be misused for reconnaissance purposes.

The Baseline and File and Print Incremental templates were the only ones from the six templates investigated that disabled unnecessary services beyond that of the default Windows 2000 server configuration. Some services such as the Task Scheduler and RunAs services could be misused to run a script or program with LocalSystem privileges and can be disabled if they are not necessary for essential server functionality. On the other hand, using the template as a starting point, a Group Policy policy could be modified to relax this OU policy to enable a service. The template also tightens the permissions on system services to further protect these services from possible manipulation from a network session even if they are enabled. The template also disables a number of services that are only set to a manual startup by a default installation, which could allow the service to later be started using a script or program that ran with enough privileges to start services. Disabling unnecessary system service is important to prevent attacks on these services that could disrupt normal functioning of a server or compromise that server's security.

There are, practically speaking, no "non security issue" hosts on a network since either computer that is compromised could be used to stage further attacks, sniff network traffic or be compromised with Trojan horse software to record keystrokes and hence passwords. The default installation of Microsoft operating software

often enables many features which can also lead to negotiation of less secure means of network communication, as in the case of SMB and Secure Channel communication, a lessened level of accountability as in the case of system auditing settings or unnecessary exposure to possible attack as in the case of unnecessary system services. The Baseline and File and Print Incremental templates when distributed using Group Policy policies on an Organizational Unit help to ensure that these system defaults are more securely and consistently configured in accordance with computer security Best Practice guidelines.

Adverse impact from the template

Since the Baseline.inf security template implements a wide range of options, some inconveniences and limitations in server functionality were experienced after the Group policy took effect on the TSTDATA1 server. The setting to prevent installation of unsigned driver software prevented the installation of a printer driver. This was corrected by changing this setting in the Group Policy policy to "Warn but allow installation". The Terminal Services service also needed to be enabled to allow remote administration of the server via Terminal Services Client. For the core functionality of a file and print server, these were the only limitations that were encountered.

While the scope of the test environment could not fully test the reasonableness of the event log settings, the requirement that the logs be cleared manually and that the server shut down if unable to log security events or if the security log reaches its maximum of 10 MB could cause real-world problems. The startup time was also monitored to measure the effect of applying the security settings though Group Policy instead of applying them to the local system policy. The result was that the server took 20 seconds longer to provide a logon screen than without the policy, which is more than acceptable. Depending on the size of the memory page file(s), the server can take longer to shut down but this time can be accommodated when conducting server maintenance.

Possible modifications to template or implementation

The Baseline.inf template provides a solid foundation for creating Group Policy polices to be to linked to Organizational Units with servers. The template was designed to be used to create an initial policy so that additional policies could be added to or relax the settings defined in the template, as was provided by the File and Print Incremental template. Based on the testing and evaluation of the baseline template, the setting regarding the installation of unsigned drivers could be changed to "Warn but allow installation." The Log on Locally User Right should also be restricted to Administrators or users that are authorized to log onto the server. The settings to shut down the server if security events can not be logged or the security log reaches its maximum size could be disabled and the clearing of Event log entries could be changed to By Days in place of manually, unless server administrators are absolutely sure to be monitoring and clearing the logs regularly or use an automated process to archive and clear the event log events. In many environments, services such as Terminal Services, Task Scheduler and Windows

Management Instrumentation may be necessary or desirable. Other services could be added to the incremental policy to ensure that they are enabled and automatically started or to tighten permissions, such as with antivirus software.

Since these settings may still subtly vary per group of servers based on their roles, different Organizational Unit structures could be used to accommodate this. One model would be to create one OU for all Servers and then within this OU, to create additional OUs for each server role such as File/Print, Application, Database, Email, Web Servers and High-Security. Then a policy based on the Baseline.inf could be applied using a policy at the Servers OU and additional policies at the server-role sub OUs. Since the Group Policy objects linked to OUs within and OU are processed after those of the parent OU, their settings will take precedence. [10] (Minasi, p.729) While security templates ease the configuration of many security-related settings in a consistent manner, Group Policy provides the mechanism to do this across multiple servers, to ensure that these settings remain configured correctly and to enable easy modification of these settings as needed.

Further research possible

In theory, any registry setting and file/registry/audit ACL on Windows servers could be set using security templates and distributed via Group Policy policies. The sceregvl.inf file defines a number of standard items to be displayed in the Security Policy and Security Configuration Analysis consoles but security templates can be edited with any text editor and can contain settings not displayed in the MMC consoles. As vulnerabilities become known for which a registry setting or tightening of permissions can help to prevent a vulnerability from being exploited, then these could be incorporated into the templates and policies used by a company. Thus, using the Baseline template as a starting point, further research could be done to investigate other settings that could be incorporated into the template and policies.

Another area of possible research is with the use of IP Security. This can be used to sign, encrypt or filter network traffic. The configuration of IP Security can also be incorporated into a company's security templates and Group Policy policies. While it is often used to encrypt network communications between clients and servers, this encryption can place a significant processing load on system CPUs, if IPsec-capable network cards are not used. This technology could be used, however, to further ensure that only authorized computers were able to communicate with a server via packet signing or filtering. One would need to research if doing so was justified given a company's computing environment and security requirements.

Conclusion

While security templates have existed for a number of years starting with the Security Configuration Manager under Windows NT, they were often difficult to distribute and maintain. The advent of Active Directory and Group Policy Objects provide the mechanism to do this efficiently. The chore remains, however, to choose a template upon which to base these policies and identify changes to a base policy or additional incremental policies that may be needed for varying server roles.

In this paper, a selection process was used to choose a security template by assigning scores to the security settings from a number of popular security templates on the basis of how much a setting's configuration added to system security relative to the impact that the configuration would have on system functionality or maintenance. Based on these criteria, the Baseline and File and Print Incremental security templates from the Microsoft Security Operations Guide offered the best balance between improving system security and minimizing the impact of that configuration. It did however result in a few problems for a test file and print server which were easily resolved by adjusting the specific security settings.

The selection and implementation of the Microsoft Baseline security template illustrates that security templates provide a good basis for a means of configuring a number of security-related settings on Windows servers. Since server roles differ as do the computing infrastructures and security requirements of companies, these templates and policies often need to be adapted to fit a company's needs. Since operating system vulnerabilities and possible exploits constantly change, these security templates and policies should also be updated regularly. Active Directory and Group Policy Objects provide the mechanism to do this efficiently and effectively.

The Baseline security template from the Microsoft Operations Guide addresses many of the core recommendations from computer security Best Practices such as enforcing a through auditing and logging of events that result from use of a server's resources, enabling of operating system options to tighten network communications and server security, and disabling unnecessary services. This is, however a trade off between system security and system functionality but the Baseline template manages to implement a stringent level of security while preserving most system functionality and can easily be modified to allow additional desired functionality. The key is to implement at least a basic security policy to ensure that a rudimentary level of system auditing and server hardening are implemented for every server on a company's network. Furthermore, it is important to remain vigilant for new exploits and to maintain these policies to further configure security settings as new settings become desirable.

References

1. Cole, Eric, Hackers Beware, Indianapolis, New Riders, 2001, p.437

2. LabMice.Net, Windows 2000 Security Checklist, http://www.labmice.net/articles/securingwin2000.htm

3. Microsoft, Microsoft Knowledge Base Article - 246261, How to Use the RestrictAnonymous Registry Value in Windows 2000, http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B246261

4. Microsoft, Microsoft Knowledge Base Article - 239869, How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT, http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B239869

5. Microsoft TechNet, Best Practices for Enterprise Security, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/bpent/bpentsec.asp

6. Microsoft TechNet, Security Operations Guide for Windows 2000 Server, 2002, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/windows2000/staysecure/default.asp

7. Microsoft, Windows 2000 Server Baseline Security Checklist, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp

8. Microsoft, Windows 2000 Server Documentation, http://www.microsoft.com/windows2000/en/server/help/

9. Minasi, Mark, et al, Mastering Windows 2000 Server, Alameda, Cybex, 2000

10. SANS Institute, The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus, Version 3.21 October 17, 2002, http://www.sans.org/top20/

Appendix A. Security Template Security Setting Comparison

	Default Server Installation	Microsoft Basic	CIS W2K Level I	Microsoft Baseline	Microsoft Secure	Microsoft HighSecure	NSA-W2K_Server
Password/Account Lockout Policy							
Enforce password history	0 passwords remembered	0 passwords remembered	24 passwords remembered	Not defined	24 passwords remembered	24 passwords remembered	24 passwords remembered
Maximum password age	42 days	42 days	90 days	Not defined	42 days	42 days	90 days
Minimum password age	0 days	0 days	1 days	Not defined	2 days	2 days	1 days
Minimum password length	0 characters	0 characters	8 characters	Not defined	8 characters	8 characters	12 characters
Passwords must meet complexity requirements	Disabled	Disabled	Enabled	Not defined	Enabled	Enabled	Enabled
Store password using reversible encryption for all users in the domain	Disabled	Disabled	Disabled	Not defined	Disabled	Disabled	Disabled
Account Lockout Policy							
Account lockout duration	Not defined	Not defined	60 minutes	Not defined	30 minutes	0	15 minutes
Account lockout threshold	0 invalid logon attempts	0 invalid logon attempts	5 invalid logon attempts	Not defined	5 invalid logon attempts	5 invalid logon attempts	3 invalid logon attempts
Reset account lockout counter after	Not defined	Not defined	60 minutes	Not defined	30 minutes	30 minutes	15 minutes
Audit Policy							
Audit account logon events	No auditing	No auditing	Success, Failure	Success, Failure	Success, Failure	Success, Failure	Success, Failure
Audit account management	No auditing	Not defined	Success, Failure	Success, Failure	Success, Failure	Success, Failure	Success, Failure
Audit directory service access	No auditing	Not defined	Not defined	Failure	Not defined	Not defined	No auditing
Audit logon events	No auditing	No auditing	Success, Failure	Success, Failure	Failure	Success, Failure	Success, Failure
Audit object access	No auditing	No auditing	Failure	Success, Failure	No auditing	Success, Failure	Failure
Audit policy change	No auditing	No auditing	Success, Failure	Success, Failure	Success, Failure	Success, Failure	Success, Failure
Audit privilege use	No auditing	No auditing	Failure	Failure	Failure	Success, Failure	Failure
Audit process tracking	No auditing	No auditing	Not defined	No auditing	No auditing	No auditing	No auditing
Audit system events	No auditing	No auditing	Success, Failure	Success, Failure	No auditing	Success, Failure	Success, Failure
User Rights Assignment							
Access this computer from the network	Backup Operators,Power Users,Users,Administrators,Ev	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators,Users

	eryone						
Act as part of the operating system		Not defined	Not defined	Not defined	Not defined	Not defined	
Add workstations to domain		Not defined	Not defined	Not defined	Not defined	Not defined	
Back up files and directories	Backup Operators,Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators
Bypass traverse checking	Backup Operators,Power Users,Users,Administrators,Everyone	Not defined	Not defined	Not defined	Not defined	Not defined	Users
Change the system time	Power Users,Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators
Create a pagefile	Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators
Create a token object		Not defined	Not defined	Not defined	Not defined	Not defined	
Create permanent shared objects		Not defined	Not defined	Not defined	Not defined	Not defined	
Debug programs	Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	
Deny access to this computer from the network		Not defined	Not defined	Not defined	Not defined	Not defined	
Deny logon as a batch job		Not defined	Not defined	Not defined	Not defined	Not defined	
Deny logon as a service		Not defined	Not defined	Not defined	Not defined	Not defined	
Deny logon locally		Not defined	Not defined	Not defined	Not defined	Not defined	
Enable computer and user accounts to be trusted for delegation		Not defined	Not defined	Not defined	Not defined	Not defined	
Force shutdown from a remote system	Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators
Generate security audits		Not defined	Not defined	Not defined	Not defined	Not defined	
Increase quotas	Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators
Increase scheduling priority	Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators
Load and unload device drivers	Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators
Lock pages in memory		Not defined	Not defined	Not defined	Not defined	Not defined	
Log on as a batch job		Not defined	Not defined	Not defined	Not defined	Not defined	
Log on as a service		Not defined	Not defined	Not defined	Not defined	Not defined	
Log on locally	Backup Operators,Power Users,Users,Administrators,STST01DA001\Guest,STST01DA001\TsInternetUser	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators

Manage auditing and security log	Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators
Modify firmware environment values	Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators
Profile single process	Power Users,Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators
Profile system performance	Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators
Remove computer from docking station	Power Users,Users,Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	
Replace a process level token		Not defined	Not defined	Not defined	Not defined	Not defined	
Restore files and directories	Backup Operators,Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators
Shut down the system	Backup Operators,Power Users,Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators
Synchronize directory service data		Not defined	Not defined	Not defined	Not defined	Not defined	
Take ownership of files or other objects	Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	Administrators
Security Options							
Additional restrictions for anonymous connections	None. Rely on default permissions	None. Rely on default permissions	No access without explicit anonymous permissions	No access without explicit anonymous permissions	Do not allow enumeration of SAM accounts and shares	No access without explicit anonymous permissions	No access without explicit anonymous permissions
Allow Automatic Administrator Logon	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined	Disabled
Allow server operators to schedule tasks (domain controllers only)	Not defined	Not defined	Not defined	Disabled	Not defined	Not defined	Not defined
Allow system to be shut down without having to log on	Disabled	Disabled	Not defined	Disabled	Not defined	Not defined	Disabled
Allowed to eject removable NTFS media	Administrators	Administrators	Not defined	Administrators	Administrators	Administrators	Administrators
Amount of idle time required before disconnecting session	15 minutes	15 minutes	15 minutes	15 minutes	15 minutes	15 minutes	30 minutes
Audit the access of global system objects	Disabled	Disabled	Not defined	Disabled	Disabled	Disabled	Enabled
Audit use of Backup and Restore privilege	Disabled	Disabled	Not defined	Disabled	Disabled	Disabled	Enabled
Automatically log off users when logon time expires (local)	Enabled	Enabled	Not defined	Enabled	Enabled	Enabled	Enabled
Clear virtual memory pagefile when system shuts down	Disabled	Disabled	Not defined	Enabled	Disabled	Enabled	Enabled
Digitally sign client communication (always)	Disabled	Disabled	Not defined	Disabled	Disabled	Enabled	Disabled
Digitally sign client communication (when possible)	Enabled	Enabled	Not defined	Enabled	Enabled	Enabled	Enabled
Digitally sign server communication (always)	Disabled	Disabled	Not defined	Enabled	Disabled	Enabled	Disabled
Digitally sign server communication (when possible)	Disabled	Disabled	Not defined	Enabled	Enabled	Enabled	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Disable Media Autoplay	Not defined	Not defined	Not defined	All Drives	Not defined	Not defined	All Drives

Do not display last user name in logon screen	Disabled	Disabled	Not defined	Enabled	Disabled	Enabled	Enabled
LAN Manager Authentication Level	Send LM & NTLM responses	Send LM & NTLM responses	Send NTLMv2 response only\refuse LM	Send NTLMv2 response only\refuse LM & NTLM	Send NTLM response only	Send NTLMv2 response only\refuse LM & NTLM	Send NTLMv2 response only\refuse LM & NTLM
Message text for users attempting to log on			This system is for the use of authorized users only. Individuals using this computer system with authority,without authority,or in excess of their authority,are subject to having all of their activities on this system monitored and recorded by system perso				Not defined
Message title for users attempting to log on			Warning: This is a monitored computer system!				Not defined
Number of previous logons to cache (in case domain controller is not available)	10 logons	10 logons	Not defined	0 logons	10 logons	10 logons	0 logons
Prevent system maintenance of computer account password	Disabled	Disabled	Not defined	Disabled	Disabled	Disabled	Disabled
Prevent users from installing printer drivers	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
Prompt user to change password before expiration	14 days	14 days	7 days	14 days	14 days	14 days	14 days
Recovery Console: Allow automatic administrative logon	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Rename administrator account	Administrator	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined
Rename guest account	Guest	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined
Restrict CD-ROM access to locally logged-on user only	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Enabled
Restrict floppy access to locally logged-on user only	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled	Disabled	Not defined	Enabled	Disabled	Enabled	Disabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled	Enabled	Not defined	Enabled	Enabled	Enabled	Enabled

Secure channel: Digitally sign secure channel data (when possible)	Enabled	Enabled	Not defined	Enabled	Enabled	Enabled	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Disabled	Disabled	Enabled	Enabled	Disabled	Enabled	Disabled
Send unencrypted password to connect to third-party SMB servers	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Shut down system immediately if unable to log security audits	Disabled	Disabled	Not defined	Enabled	Disabled	Disabled	Enabled
Smart card removal behavior	No Action	No Action	Not defined	Lock Workstation	Lock Workstation	Lock Workstation	Lock Workstation
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
Unsigned driver installation behavior	Warn but allow installation	Not defined	Warn but allow installation	Do not allow installation	Warn but allow installation	Do not allow installation	Warn but allow installation
Unsigned non-driver installation behavior	Silently succeed	Not defined	Warn but allow installation	Warn but allow installation	Silently succeed	Silently succeed	Warn but allow installation
Settings for Event logs							
Maximum application log size	512 kilobytes	512 kilobytes	Not defined	10240 kilobytes	Not defined	Not defined	4194240 kilobytes
Maximum security log size	512 kilobytes	512 kilobytes	Not defined	10240 kilobytes	5120 kilobytes	10240 kilobytes	4194240 kilobytes
Maximum system log size	512 kilobytes	512 kilobytes	Not defined	10240 kilobytes	Not defined	Not defined	4194240 kilobytes
Restrict guest access to application log	Disabled	Disabled	Not defined	Enabled	Enabled	Enabled	Enabled
Restrict guest access to security log	Disabled	Disabled	Not defined	Enabled	Enabled	Enabled	Enabled
Restrict guest access to system log	Disabled	Disabled	Not defined	Enabled	Enabled	Enabled	Enabled
Retain application log	7 days	7 days	Not defined	Not defined	Not defined	Not defined	7 days
Retain security log	7 days	7 days	Not defined	Not defined	Not defined	Not defined	7 days
Retain system log	7 days	7 days	Not defined	Not defined	Not defined	Not defined	7 days
Retention method for application log	By days	By days	Not defined	Manually	Not defined	Not defined	Manually
Retention method for security log	By days	By days	Not defined	Manually	As needed	As needed	Manually
Retention method for system log	By days	By days	Not defined	Manually	Not defined	Not defined	Manually
Shut down the computer when the security audit log is full	Disabled	Disabled	Not defined	Enabled	Not defined	Not defined	Enabled
Restricted groups							
Administrators	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined
Backup Operators	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined
Guests	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined
Power Users	Not defined	Not defined	Not defined	Not defined	OK	Not defined	OK
Replicator	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined
Users	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined
System Services							
Alerter	OK	OK	Investigate	Investigate	Not defined	Not defined	Not defined
Application Management	OK	OK	Not defined	Investigate	Not defined	Not defined	Not defined
Automatic Updates	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined

Background Intelligent Transfer Service	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined
ClipBook	OK	OK	Investigate	Investigate	Not defined	Not defined	Not defined
COM+ Event System	Not defined	Not defined	Not defined	OK	Not defined	Not defined	Not defined
Computer Browser	OK	OK	Not defined	Investigate	Not defined	Not defined	Not defined
DHCP Client	OK	OK	Not defined	OK	Not defined	Not defined	Not defined
Distributed File System	OK	OK	Not defined	Investigate	Not defined	Not defined	Not defined
Distributed Link Tracking Client	OK	OK	Not defined	OK	Not defined	Not defined	Not defined
Distributed Link Tracking Server	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
Distributed Transaction Coordinator	OK	OK	Not defined	Investigate	Not defined	Not defined	Not defined
DNS Client	OK	OK	Not defined	OK	Not defined	Not defined	Not defined
Event Log	OK	OK	Not defined	OK	Not defined	Not defined	Not defined
Fax Service	Not defined	Not defined	Investigate	Investigate	Not defined	Not defined	Not defined
File Replication	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
Indexing Service	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
Internet Connection Sharing	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
Intersite Messaging	Not defined	Not defined	Not defined	OK	Not defined	Not defined	Not defined
IPSEC Policy Agent	OK	OK	Not defined	Investigate	Not defined	Not defined	Not defined
Kerberos Key Distribution Center	Not defined	Not defined	Not defined	OK	Not defined	Not defined	Not defined
License Logging Service	OK	OK	Not defined	Investigate	Not defined	Not defined	Not defined
Logical Disk Manager	OK	OK	Not defined	OK	Not defined	Not defined	Not defined
Logical Disk Manager Administrative Service	Not defined	Not defined	Not defined	OK	Not defined	Not defined	Not defined
Messenger	OK	OK	Investigate	Investigate	Not defined	Not defined	Not defined
Net Logon	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
NetMeeting Remote Desktop Sharing	Not defined	Not defined	Investigate	Investigate	Not defined	Not defined	Not defined
Network Connections	Not defined	Not defined	Not defined	OK	Not defined	Not defined	Not defined
Network DDE	OK	OK	Not defined	Investigate	Not defined	Not defined	Not defined
Network DDE DSDM	OK	OK	Not defined	Investigate	Not defined	Not defined	Not defined
NT LM Security Support Provider	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
Performance Logs and Alerts	Not defined	Not defined	Not defined	OK	Not defined	Not defined	Not defined
Plug and Play	OK	OK	Not defined	OK	Not defined	Not defined	Not defined
Print Spooler	OK	OK	Not defined	OK	Not defined	Not defined	Not defined
Protected Storage	OK	OK	Not defined	OK	Not defined	Not defined	Not defined
QoS RSVP	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
Remote Access Auto Connection Manager	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
Remote Access Connection Manager	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
Remote Procedure Call (RPC)	OK	OK	Not defined	OK	Not defined	Not defined	Not defined
Remote Procedure Call (RPC) Locator	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
Remote Registry Service	OK	OK	Not defined	OK	Not defined	Not defined	Not defined
Removable Storage	OK	OK	Not defined	Investigate	Not defined	Not defined	Not defined
Routing and Remote Access	Not defined	Not defined	Not defined	OK	Not defined	Not defined	Not defined

RunAs Service	OK	OK	Not defined	Investigate	Not defined	Not defined	Not defined
Security Accounts Manager	OK	OK	Not defined	OK	Not defined	Not defined	Not defined
Server	OK	OK	Not defined	OK	Not defined	Not defined	Not defined
Smart Card	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
Smart Card Helper	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
System Event Notification	OK	OK	Not defined	OK	Not defined	Not defined	Not defined
Task Scheduler	OK	OK	Not defined	Investigate	Not defined	Not defined	Not defined
TCP/IP NetBIOS Helper Service	OK	OK	Not defined	OK	Not defined	Not defined	Not defined
Telephony	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
Telnet	Not defined	Not defined	Investigate	Investigate	Not defined	Not defined	Not defined
Terminal Services	Not defined	Not defined	Not defined	OK	Not defined	Not defined	Not defined
Uninterruptible Power Supply	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
Utility Manager	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
VMware Tools Service	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined	Not defined
Windows Installer	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
Windows Management Instrumentation	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
Windows Management Instrumentation Driver Extensions	Not defined	Not defined	Not defined	OK	Not defined	Not defined	Not defined
Windows Time	Not defined	Not defined	Not defined	Investigate	Not defined	Not defined	Not defined
Workstation	OK	OK	Not defined	OK	Not defined	Not defined	Not defined

Appendix B. Security Template Selection Scoring

Scores range from 1 to 5, based on how much security a setting adds to the default value relative to the impact it has on system performance or function. A score of 0 indicates that a setting is equal to the default or not applicable.

	Microsoft Basic	CIS W2K Level I	Microsoft Baseline	Microsoft Secure	Microsoft HighSecure	NSA-W2K_Server
Password and Account Policy	0	4	0	3	3	5
Audit Policy	0	3	4	3	4	4
User Rights Assignment	0	0	0	0	0	1
Security Options						
Additional restrictions for anonymous connections	0	4	4	3	4	4
Allow Automatic Administrator Logon	0	0	0	0	0	1
Allow server operators to schedule tasks (domain controllers only)	0	0	0	0	0	0
Allow system to be shut down without having to log on	0	0	0	0	0	0
Allowed to eject removable NTFS media	0	0	0	0	0	0
Amount of idle time required before disconnecting session	0	0	0	0	0	1
Audit the access of global system objects	0	0	0	0	0	0
Audit use of Backup and Restore privilege	0	0	0	0	0	2
Automatically log off users when logon time expires (local)	0	0	0	0	0	0
Clear virtual memory pagefile when system shuts down	0	0	4	0	4	4
Digitally sign client communication (always)	0	0	0	0	2	0
Digitally sign client communication (when possible)	0	0	0	0	0	0
Digitally sign server communication (always)	0	0	1	0	1	0
Digitally sign server communication (when possible)	0	0	3	3	3	3
Disable CTRL+ALT+DEL requirement for logon	0	0	0	0	0	0
Disable Media Autoplay	0	0	1	0	0	1
Do not display last user name in logon screen	0	0	1	0	1	1
LAN Manager Authentication Level	0	3	4	2	4	4
Message text for users attempting to log on	0	0	0	0	0	0
Message title for users attempting to log on	0	0	0	0	0	0
Number of previous logons to cache (in case domain controller is not available)	0	0	4	0	0	4
Prevent system maintenance of computer account password	0	0	0	0	0	0
Prevent users from installing printer drivers	0	0	0	0	0	0
Prompt user to change password before expiration	0	1	0	0	0	0
Recovery Console: Allow automatic administrative logon	0	0	0	0	0	0
Recovery Console: Allow floppy copy and access to all drives and all folders	0	0	0	0	0	0

Rename administrator account	0	0	0	0	0	0
Rename guest account	0	0	0	0	0	0
Restrict CD-ROM access to locally logged-on user only	0	3	3	0	0	3
Restrict floppy access to locally logged-on user only	0	3	3	0	0	3
Secure channel: Digitally encrypt or sign secure channel data (always)	0	0	1	0	1	0
Secure channel: Digitally encrypt secure channel data (when possible)	0	0	0	0	0	0
Secure channel: Digitally sign secure channel data (when possible)	0	0	0	0	0	0
Secure channel: Require strong (Windows 2000 or later) session key	0	4	4	0	4	0
Send unencrypted password to connect to third-party SMB servers	0	0	0	0	0	0
Shut down system immediately if unable to log security audits	0	0	1	0	0	1
Smart card removal behavior	0	0	1	1	1	1
Strengthen default permissions of global system objects (e.g. Symbolic Links)	0	0	0	0	0	0
Unsigned driver installation behavior	0	0	1	0	1	0
Unsigned non-driver installation behavior	0	1	1	0	0	1
Settings for Event logs						
Maximum application log size	0	0	4	0	0	1
Maximum security log size	0	0	4	3	3	1
Maximum system log size	0	0	4	0	0	1
Restrict guest access to application log	0	0	4	4	4	4
Restrict guest access to security log	0	0	4	4	4	4
Restrict guest access to system log	0	0	4	4	4	4
Retain application log	0	0	0	0	0	0
Retain security log	0	0	0	0	0	0
Retain system log	0	0	0	0	0	0
Retention method for application log	0	0	1	0	0	1
Retention method for security log	0	0	1	0	0	1
Retention method for system log	0	0	1	0	0	1
Shut down the computer when the security audit log is full	0	0	1	0	0	1
Restricted groups	0	0	0	1	0	1
System Services	0	0	2	0	0	0
TOTAL	0	26	71	31	48	64