the CENTER for INTERNET SECURITY

Windows Server 2003

Operating System

Legacy, Enterprise, and Specialized Security Benchmark Consensus Security Settings for Domain Controllers

Version 2.0

November 2007

http://www.cisecurity.org

Editors: Jeff Shawgo
Sidney Faber
Collin Greene
windows-feedback@cisecurity.org

Table of Contents

Terms of Use Agreement

Background.

The Center for Internet Security ("**CIS**") provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere (“**Products**”) as a public service to Internet users worldwide. Recommendations contained in the Products (“**Recommendations**”) result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems, and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a “quick fix” for anyone’s information security needs.

No Representations, Warranties, or Covenants.

CIS makes no representations, warranties, or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness, or completeness of the Products or the Recommendations. CIS is providing the Products and the Recommendations “as is” and “as available” without representations, warranties, or covenants of any kind.

User Agreements.

By using the Products and/or the Recommendations, I and/or my organization (“**We**”) agree and acknowledge that:

1. No network, system, device, hardware, software, or component can be made fully secure;
2. We are using the Products and the Recommendations solely at our own risk;
3. We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS’s negligence or failure to perform;
4. We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;
5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades, or bug fixes; or to notify us of the need for any such corrections, updates, upgrades, or bug fixes; and
6. Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of

use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of Limited Rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

1. Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;
2. Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of Intellectual Property Rights; Limitations on Distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled “Grant of limited rights.”

Subject to the paragraph entitled “Special Rules” (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend, and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development, or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs, and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special Rules.

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (http://nsa2.www.conxion.com/cisco/notice.htm).

CIS has created and will from time to time create, special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of Law; Jurisdiction; Venue

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.

WE ACKNOWLEDGE THAT WE HAVE READ THESE AGREED TERMS OF USE IN THEIR ENTIRETY, UNDERSTAND THEM, AND WE AGREE TO BE BOUND BY THEM IN ALL RESPECTS.

Quick Start Instructions

Just a few years ago, it was almost impossible to find a reliable source for Windows security. Since then, the momentum has shifted in the opposite direction – there is a wealth of information available. Now the questions are, "Which published source do I trust as authoritative? What should MY standard be?"

One side-effect of this wealth of information available is that there are local computer security experts who want to toss the documentation aside, and apply the standards. I have one piece of advice before you go and do that:

IF YOU ONLY READ ONE PAGE IN THIS GUIDE, READ THIS PAGE!

This guide imposes changes that are best implemented in a managed environment. They are designed to limit communication between computers to positively identified and authorized personnel. This is a change from the normal way of thinking in a Windows world. Major systems should still function, but testing this benchmark in a controlled environment is essential.

For The Seasoned Security Professional

More and more Windows support personnel are becoming familiar with the intricacies of Windows security. Microsoft itself has stated an organizational shift of its priorities away from ease-of-use toward security awareness.

Section 1 of this guide is a summary checklist of the configuration settings that constitute a Windows Server compliant computer system. Appendix A is a questionnaire that can be used to put the trade-offs into perspective for each of the settings involved.

For the Windows User Seeking Enlightenment

Computer and network security is a difficult topic to summarize. Many of the features that are enabled "out of the box" on a Windows computer are enabled "in case" the prospective owner wants to use them. Most of these features never get used, but often still have vulnerabilities that can be exploited by unscrupulous people.

Section 2 of this guide is written to provide contextual descriptions of each requirement for this benchmark. It gives plain-text details of what the setting means, why it is restricted, and what the consequences of restricting that setting may be. It covers the same information as Section 1, in greater detail. You should still use the questionnaire in Appendix A to explore some of the trade-offs of implementing these settings.

Windows Server 2003 – Domain Controller Benchmark Consensus Baseline Security Settings

This document is a security benchmark for the Microsoft Windows Server 2003 operating system for domain members. It reflects the content of the Consensus Baseline Security Settings document developed by the National Security Agency (NSA), the Defense Information Systems Agency (DISA), The National Institute of Standards and Technology (NIST), the General Services Administration (GSA), The SANS Institute, and the staff and members of the Center for Internet Security (CIS).

Intended Audience

This benchmark is intended for anyone using a Windows Server 2003 operating system who feels at all responsible for the security of that system. A Security Manager or Information Security Officer should certainly be able to use this guide and the associated tools to gather information about the security status of a network of Windows machines. The owner of a small business or home office can use this guide as a straightforward aid in enhancing his or her own personal network security. A Windows System Administrator can use this guide and the associated tools to produce explicit scores that can be given to management to reflect where they currently stand, versus where they should stand with regard to security.

Any user who uses this guide to make even the slightest improvement on the secure state of a system might be doing just enough to turn a potential hacker or cracker away to an easier target. Every computer operator who becomes “Security Aware” improves the safety level of the Internet.

Practical Application

Just as there is often no single correct way to get to a specific destination, there is more than one way to implement the settings and suggestions described in this text. In a network environment, with a Windows 2000 or Windows 2003 Active Directory Domain, Group Policy can be used to apply nearly all the settings described herein. Many surveys of Fortune 500 or Fortune 1000 companies have indicated that large companies have been slow to migrate to Active Directory because of the level of complexity involved, but the lack of continued support for Windows NT 4.0 Domains is fueling the migration process. Once an infrastructure has been implemented to support an Active Directory domain, implementing most of these policies with Group Policy becomes relatively easy.

The Local Security Policy editor of individual Servers and Workstations can also be used to lock down their environment.

The information contained in this text applies equally well to Local Security Policies and to Group Policies. In a large domain infrastructure, Group Policy can (and should) be set to override the Local Security Policy. Anyone attempting to make modifications to the Local Security Policy which seem to “mysteriously disappear” should contact their system administrator or their management to see if Group Policy may be overriding their changes.

The actions required to securely configure a Windows operating system will be described in terms of updating the Local Security Policy. The Local Security Policy Editor, as well as many other tools used herein, is located in the Administrative Tools menu. In some cases, clicking the Start button, and then looking under Programs will be enough. Otherwise, click Start, Settings, and open the Control Panel. Double-click the Administrative Tools icon in the Control Panel to find the Local Security Policy Editor.

Keeping Score

The goal of every benchmark and the associated scoring tools is to give users a point-in-time view of where systems stand in relation to the currently accepted standard. This “score” produced by the scoring tool is a number between zero and ten, and is derived from the table below.

The criteria used for scoring are divided into five categories: (1) Service Packs and Security Updates, (2) Auditing and Account Policies, (3) Security Settings, (4) Additional Security Protection, and (5) Administrative Templates. Additional applications or Services may detract from the overall score, just as additional services detract from the security of these systems in the production environment.

Security Levels

One question that needs to be considered when securing computers is "How secure should they be?" Often people assume that the highest level of security is best, but it is important to remember that often, a vulnerability is defended by disabling some functionality. The use of this function may be more important to the usefulness of the computer than defending against the vulnerability.

In response to this, CIS is publishing three different levels of guidance.

Legacy - Settings in this level are designed for domain controllers that need to operate with older systems such as Windows NT, or in environments where older third party applications are required. The settings will not affect the function or performance of the operating system or of applications that are running on the system.

Enterprise - Settings in this level are designed for domain controllers operating in a managed environment where interoperability with legacy systems is not required. It assumes that all operating systems within the enterprise are Windows 2000 or later, therefore able to use all possible security features available within those systems. In such environments, these Enterprise-level settings are not likely to affect the function or performance of the OS. However, one should carefully consider the possible impact to software applications when applying these recommended technical controls.

Specialized Security – Limited Functionality – Formerly "High Security," settings in this level are designed for domain controllers in which security and integrity are the highest priorities, even at the expense of functionality, performance, and interoperability. Therefore, each setting should be considered carefully and only applied by an experienced administrator who has a thorough understanding of the potential impact of each setting or action in a particular environment.

Section 1 – Summary Checklist

Setting:	Legacy	Enterprise	Specialized Security – Limited Functionality
1 Service Packs and Hotfixes			
1.1 Major Service Pack and Hotfix Requirements			
1.1.1 Current Service Pack Installed	SP2		
1.2 Minor Service Pack and Hotfix Requirements			
1.2.1 Hotfixes recognized by HFNetChk	All Critical and Important Hotfixes		
2 Auditing and Account Policies			
2.1 Major Auditing and Account Policies Requirements			
2.1.1 Minimum Password Length	8 Characters		12 Characters
2.1.2 Maximum Password Age	42 Days		
2.2 Minor Auditing and Account Policies Requirements			
2.2.1 Audit Policy (minimums)			
2.2.1.1 Audit Account Logon Events	Success and Failure		
2.2.1.2 Audit Account Management	Success and Failure		
2.2.1.3 Audit Directory Service Access	<Not Defined>		
2.2.1.4 Audit Logon Events	Success and Failure		
2.2.1.5 Audit Object Access	Success and Failure		
2.2.1.6 Audit Policy Change	Success (minimum)		
2.2.1.7 Audit Privilege Use	<Not Defined>		
2.2.1.8 Audit Process Tracking	<Not Defined>		
2.2.1.9 Audit System Events	Success (minimum)		
2.2.2 Account Policy			
2.2.2.1 Minimum Password Age	1 day		
2.2.2.2 Maximum Password Age	42 days		
2.2.2.3 Minimum Password Length	8 characters		12 characters
2.2.2.4 Password Complexity	Enabled		
2.2.2.5 Password History	24 passwords remembered		
2.2.2.6 Store Passwords using Reversible Encryption	Disabled		

Setting:	**Legacy**	**Enterprise**	**Specialized Security – Limited Functionality**
2.2.3 Account Lockout Policy			
2.2.3.1 Account Lockout Duration	15 minutes		15 minutes
2.2.3.2 Account Lockout Threshold	15 attempts		10 attempts
2.2.3.3 Reset Account Lockout After	15 minutes		15 minutes
2.2.4 Event Log Settings – Application, Security, and System Logs			
2.2.4.1 Application Log			
2.2.4.1.1 Maximum Event Log Size	16 MB		
2.2.4.1.2 Restrict Guest Access	Enabled		
2.2.4.1.3 Log Retention Method	<Not Defined>		
2.2.4.1.4 Log Retention	<Not Defined>		
2.2.4.2 Security Log			
2.2.4.2.1 Maximum Event Log Size	80 MB		
2.2.4.2.2 Restrict Guest Access	Enabled		
2.2.4.2.3 Log Retention Method	<Not Defined>		
2.2.4.2.4 Log Retention	<Not Defined>		
2.2.4.3 System Log			
2.2.4.3.1 Maximum Event Log Size	16 MB		
2.2.4.3.2 Restrict Guest Access	Enabled		
2.2.4.3.3 Log Retention Method	<Not Defined>		
2.2.4.3.4 Log Retention	<Not Defined>		

<table>
<tr><th>Setting:</th><th>Legacy</th><th>Enterprise</th><th>Specialized Security – Limited Functionality</th></tr>
<tr><td colspan="4">3 Security Settings</td></tr>
<tr><td colspan="4">3.1 Major Security Settings</td></tr>
<tr><td>3.1.1 Network Access: Allow Anonymous SID/Name Translation:</td><td>&lt;Not Defined&gt;</td><td colspan="2">Disabled</td></tr>
<tr><td>3.1.2 Network Access: Do not allow Anonymous Enumeration of SAM Accounts</td><td>&lt;Not Defined&gt;</td><td colspan="2">Enabled</td></tr>
<tr><td>3.1.3 Network Access: Do not allow Anonymous Enumeration of SAM Accounts and Shares</td><td>&lt;Not Defined&gt;</td><td colspan="2">Enabled</td></tr>
<tr><td colspan="4">3.2 Minor Security Settings</td></tr>
<tr><td colspan="4">3.2.1 Security Options</td></tr>
<tr><td>3.2.1.1 Accounts: Administrator Account Status</td><td colspan="3">&lt;Not Defined&gt;</td></tr>
<tr><td>3.2.1.2 Accounts: Guest Account Status</td><td colspan="3">Disabled</td></tr>
<tr><td>3.2.1.3 Accounts: Limit local account use of blank passwords to console logon only</td><td colspan="3">Enabled</td></tr>
<tr><td>3.2.1.4 Accounts: Rename Administrator Account</td><td colspan="3">&lt;non-standard&gt;</td></tr>
<tr><td>3.2.1.5 Accounts: Rename Guest Account</td><td colspan="3">&lt;non-standard&gt;</td></tr>
<tr><td>3.2.1.6 Audit: Audit the access of global system objects</td><td colspan="3">&lt;Not Defined&gt;</td></tr>
<tr><td>3.2.1.7 Audit: Audit the use of backup and restore privilege</td><td colspan="3">&lt;Not Defined&gt;</td></tr>
<tr><td>3.2.1.8 Audit: Shut Down system immediately if unable to log security alerts</td><td colspan="2">&lt;Not Defined&gt;</td><td>Enabled</td></tr>
<tr><td>3.2.1.9 DCOM: Machine Access Restrictions in Security Descriptor Definition Language</td><td colspan="2">&lt;Not Defined&gt;</td><td>&lt;Not Defined&gt;</td></tr>
<tr><td>3.2.1.10 DCOM: Machine Launch</td><td colspan="2">&lt;Not Defined&gt;</td><td>&lt;Not Defined&gt;</td></tr>
</table>

Setting:	**Legacy**	**Enterprise**	**Specialized Security – Limited Functionality**
Restrictions in Security Descriptor Definition Language			
3.2.1.11 Devices: Allow undock without having to log on	<Not Defined>		
3.2.1.12 Devices: Allowed to format and eject removable media	Administrators		
3.2.1.13 Devices: Prevent users from installing printer drivers	Enabled		
3.2.1.14 Devices: Restrict CD-ROM Access to Locally Logged-On User Only	<Not Defined>		
3.2.1.15 Devices: Restrict Floppy Access to Locally Logged-On User Only	<Not Defined>		
3.2.1.16 Devices: Unsigned Driver Installation Behavior	“Warn, but allow…”		
3.2.1.17 Domain Controller: Allow Server Operators to Schedule Tasks	<Disabled>		
3.2.1.18 Domain Controller: LDAP Server Signing Requirements	<Not Defined>		Require Signing
3.2.1.19 Domain Controller: Refuse machine account password changes	<Disabled>		
3.2.1.20 Domain Member: Digitally Encrypt or Sign Secure Channel Data (Always)	<Not Defined>		
3.2.1.21 Domain Member: Digitally Encrypt Secure Channel Data (When Possible)	Enabled		
3.2.1.22 Domain Member: Digitally Sign Secure Channel Data (When Possible)	Enabled		
3.2.1.23 Domain Member: Disable Machine Account Password Changes	Disabled		
3.2.1.24 Domain Member: Maximum Machine Account Password Age	30 days		
3.2.1.25 Domain Member: Require Strong (Windows 2000 or later) Session Key	Enabled		

<table>
<tr><th>Setting:</th><th>Legacy</th><th>Enterprise</th><th>Specialized Security – Limited Functionality</th></tr>
<tr><td>3.2.1.26 Interactive Logon: Do Not Display Last User Name</td><td colspan="3">Enabled</td></tr>
<tr><td>3.2.1.27 Interactive Logon: Do not require CTRL+ALT+DEL</td><td colspan="3">Disabled</td></tr>
<tr><td>3.2.1.28 Interactive Logon: Message Text for Users Attempting to Log On</td><td colspan="3"><Custom, or DoJ Approved></td></tr>
<tr><td>3.2.1.29 Interactive Logon: Message Title for Users Attempting to Log On</td><td colspan="3"><Custom, or DoJ Approved></td></tr>
<tr><td>3.2.1.30 Interactive Logon: Number of Previous Logons to Cache</td><td colspan="3"><Not Defined></td></tr>
<tr><td>3.2.1.31 Interactive Logon: Prompt User to Change Password Before Expiration</td><td colspan="3">14 days</td></tr>
<tr><td>3.2.1.32 Interactive Logon: Require Domain Controller authentication to unlock workstation</td><td colspan="3">Enabled.</td></tr>
<tr><td>3.2.1.33 Interactive logon: Require smart card</td><td colspan="3"><Not Defined></td></tr>
<tr><td>3.2.1.34 Interactive Logon: Smart Card Removal Behavior</td><td colspan="3">Lock Workstation</td></tr>
<tr><td>3.2.1.35 Microsoft Network Client: Digitally sign communications (always)</td><td><Not Defined></td><td colspan="2">Enabled</td></tr>
</table>

Setting:	Legacy	Enterprise	Specialized Security – Limited Functionality
3.2.1.36 Microsoft Network Client: Digitally sign communications (if server agrees)	Enabled		
3.2.1.37 Microsoft Network Client: Send Unencrypted Password to Connect to Third-Part SMB Server	Disabled		
3.2.1.38 Microsoft Network Server: Amount of Idle Time Required Before Disconnecting Session	15 Minutes		
3.2.1.39 Microsoft Network Server: Digitally sign communications (always)	<Not Defined>		
3.2.1.40 Microsoft Network Server: Digitally sign communications (if client agrees)	Enabled		
3.2.1.41 Microsoft Network Server: Disconnect clients when logon hours expire	Enabled		
3.2.1.42 Network Access: Do not allow storage of credentials or .NET passports for network authentication	Enabled.	Enabled	
3.2.1.43 Network Access: Let Everyone permissions apply to anonymous users	Disabled		
3.2.1.44 Network Access: Named pipes that can be accessed anonymously	<None>		
3.2.1.45 Network Access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\WindowsNT\CurrentVersion		

Setting:	Legacy	Enterprise	Specialized Security – Limited Functionality
3.2.1.46 Network Access: Remotely accessible registry paths and subpaths	Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog		
3.2.1.47 Network access: Restrict anonymous access to Named Pipes and Shares	Enabled		
3.2.1.48 Network Access: Shares that can be accessed anonymously	<None>		
3.2.1.49 Network Access: Sharing and security model for local accounts	Classic		
3.2.1.50 Network Security: Do not store LAN Manager password hash value on next password change	<Not Defined>	Enabled	
3.2.1.51 Network Security: Force logoff when logon hours expire	<Not Defined>		
3.2.1.52 Network Security: LAN Manager Authentication Level	Send NTLMv2	Send NTLMv2, refuse LM	Send NTLMv2, refuse LM and NTLM
3.2.1.53 Network Security: LDAP client signing requirements	Negotiate Signing or Require Signing		
3.2.1.54 Network Security: Minimum session security for NTLM SSP based (including secure RPC) clients	<Not Defined>	Require Message Integrity, Message Confidentiality, NTLMv2 Session Security, 128-bit Encryption	

Setting:	**Legacy**	**Enterprise**	**Specialized Security – Limited Functionality**
3.2.1.55 Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers	<Not Defined>	Require Message Integrity, Message Confidentiality, NTLMv2 Session Security, 128-bit Encryption	
3.2.1.56 Recovery Console: Allow Automatic Administrative Logon	Disabled		
3.2.1.57 Recovery Console: Allow Floppy Copy and Access to All Drives and All Folders	<Not Defined>		
3.2.1.58 Shutdown: Allow System to be Shut Down Without Having to Log On	Disabled		
3.2.1.59 Shutdown: Clear Virtual Memory Pagefile	<Not Defined>		
3.2.1.60 System cryptography: Force strong key protection for user keys stored on the computer	User must enter a password each time they use a key		
3.2.1.61 System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	<Not Defined>		
3.2.1.62 System objects: Default owner for objects created by members of the Administrators group	Object Creator		
3.2.1.63 System objects: Require case insensitivity for non-Windows subsystems	<Not Defined>		
3.2.1.64 System objects: Strengthen default permissions of internal system objects	Enabled		
3.2.1.65 System settings: Optional subsystems	<None>		

Setting:	Legacy	Enterprise	Specialized Security – Limited Functionality
3.2.1.66 System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	<Not Defined>		
3.2.1.67 MSS: (AFD DynamicBacklogGrowthDelta) Number of connections to create when additional connections are necessary for Winsock applications (10 recommended)	10		
3.2.1.68 MSS: (AFD EnableDynamicBacklog) Enable dynamic backlog for Winsock applications (recommended)	Enabled		
3.2.1.69 MSS: (AFD MaximumDynamicBacklog) Maximum number of 'quasi-free' connections for Winsock applications	20000		
3.2.1.70 MSS: (AFD MinimumDynamicBacklog) Minimum number of free connections for Winsock applications (20 recommended for systems under attack, 10 otherwise)	20		
3.2.1.71 MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	Highest Protection, source routing is automatically disabled.		
3.2.1.72 MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)	Disabled		

Setting:	Legacy	Enterprise	Specialized Security – Limited Functionality
3.2.1.73 MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	Disabled		
3.2.1.74 MSS: (EnablePMTUDiscovery) Allow automatic detection of MTU size (possible DoS by an attacker using a small MTU)	<Not Defined>		Enabled
3.2.1.75 MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	Enabled		
3.2.1.76 MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure DefaultGateway addresses (could lead to DoS)	Disabled		
3.2.1.77 MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)	Connections time out sooner if a SYN attack is detected		
3.2.1.78 MSS: (TCPMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged	3 & 6 seconds, half-open connections dropped after 21 seconds		
3.2.1.79 MSS: (TCPMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	3		

<table>
<tr><th>Setting:</th><th>Legacy</th><th>Enterprise</th><th>Specialized Security – Limited Functionality</th></tr>
<tr><td>3.2.1.80 MSS: (TCPMaxPortsExhausted) How many dropped connect requests to initiate SYN attack protection (5 is recommended)</td><td colspan="3">5</td></tr>
<tr><td>3.2.1.81 MSS: Disable Autorun for all drives</td><td colspan="3">255, disable autorun for all drives</td></tr>
<tr><td>3.2.1.82 MSS: Enable Safe DLL search mode</td><td colspan="3">Enabled</td></tr>
<tr><td>3.2.1.83 MSS: Enable the computer to stop generating 8.3 style filenames</td><td colspan="2"><Not Defined></td><td>Enabled</td></tr>
<tr><td>3.2.1.84 MSS: How often keep-alive packets are sent in milliseconds</td><td colspan="3">300000</td></tr>
<tr><td>3.2.1.85 MSS: Percentage threshold for the security event log at which the system will generate a warning</td><td colspan="3"><Not Defined></td></tr>
<tr><td>3.2.1.86 MSS: The time in seconds before the screen saver grace period expires</td><td colspan="3">0</td></tr>
</table>

Setting:	**Legacy**	**Enterprise**	**Specialized Security – Limited Functionality**
4 Additional Security Protection			
4.1 Available Services (Permissions on services listed here: Administrators: Full Control; System: Full Control; Interactive: Read)			
4.1.1 Alerter	Disabled		
4.1.2 Client Services for Netware	Disabled		
4.1.3 Clipbook	Disabled		
4.1.4 Fax Service	Disabled		
4.1.5 File Replication	Disabled		
4.1.6 File Services for Macintosh	Disabled		
4.1.7 FTP Publishing Service	Disabled		
4.1.8 Help and Support	Disabled		
4.1.9 HTTP SSL	Disabled		
4.1.10 IIS Admin Service	Disabled		
4.1.11 Indexing Service	Disabled		
4.1.12 License Logging Service	Disabled		
4.1.13 Messenger	Disabled		
4.1.14 Microsoft POP3 Service	Disabled		
4.1.15 NetMeeting Remote Desktop Sharing	Disabled		
4.1.16 Network Connections	Manual		
4.1.17 Network News Transport Protocol (NNTP)	Disabled		
4.1.18 Print Server for Macintosh	Disabled		
4.1.19 Print Spooler	<Not Defined>		Disabled
4.1.20 Remote Access Auto Connection Manager	Disabled		
4.1.21 Remote Access Connection Manager	Disabled		
4.1.22 Remote Administration Service	Disabled		
4.1.23 Remote Desktop Help Session Manager	Disabled		
4.1.24 Remote Installation	Disabled		
4.1.25 Remote Procedure Call (RPC) Locator	Disabled		
4.1.26 Remote Registry Service	<Not Defined>		Disabled

Setting:	Legacy	Enterprise	Specialized Security – Limited Functionality
4.1.27 Remote Server Manager	Disabled		
4.1.28 Remote Server Monitor	Disabled		
4.1.29 Remote Storage Notification	Disabled		
4.1.30 Remote Storage Server	Disabled		
4.1.31 Simple Mail Transfer Protocol (SMTP)	Disabled		
4.1.32 Simple Network Management Protocol (SNMP) Service	Disabled		
4.1.33 Simple Network Management Protocol (SNMP) Trap	Disabled		
4.1.34 Telephony	Disabled		
4.1.35 Telnet	Disabled		
4.1.36 Terminal Services	<Not Defined>		Disabled
4.1.37 Trivial FTP Daemon	Disabled		
4.1.38 Volume Shadow Service	Enabled.		
4.1.39 Wireless Configuration	Disabled		
4.1.40 World Wide Web Publishing Services	Disabled		
4.1.41 Windows Media Server	Disabled.		
4.1.42 Data Execution Prevention	Enabled.		
4.2 User Rights			
4.2.1 Access this computer from the network	<Not Defined>		Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS
4.2.2 Act as part of the operating system	<None>		
4.2.3 Add workstations to domain	<Not Defined>		<None>
4.2.4 Adjust memory quotas for a process	<Not Defined>		NETWORK SERVICE, LOCAL SERVICE, Administrators
4.2.5 Allow log on locally	Administrators		
4.2.6 Allow logon through terminal services	Administrators		
4.2.7 Back up files and directories	<Not Defined>		

Setting:	**Legacy**	**Enterprise**	**Specialized Security – Limited Functionality**
4.2.8 Bypass traverse checking	<Not Defined>		
4.2.9 Change the system time	Administrators		
4.2.10 Create a pagefile	<Not Defined>		Administrators
4.2.11 Create a token object	<None>		
4.2.12 Create Global Objects	<Not Defined>		
4.2.13 Create permanent shared objects	<None>		
4.2.14 Debug Programs	<None>		
4.2.15 Deny access to this computer from the network (minimum)	<Not Defined>		ANONOYMOUS LOGON, Guests
4.2.16 Deny logon as a batch job	<Not Defined>		
4.2.17 Deny logon as a service	<Not Defined>		
4.2.18 Deny logon locally	<Not Defined>		
4.2.19 Deny logon through Terminal Service (minimum)	<Not Defined>		
4.2.20 Enable computer and user accounts to be trusted for delegation	<None>		
4.2.21 Force shutdown from a remote system	<Not Defined>		Administrators
4.2.22 Generate security audits	<Not Defined>		Local Service, Network Service
4.2.23 Impersonate a client after authentication	SERVICE		
4.2.24 Increase scheduling priority	<Not Defined>		Administrators
4.2.25 Load and unload device drivers	Administrators		
4.2.26 Lock pages in memory	<Not Defined>		Administrators
4.2.27 Log on as a batch job	<None>		
4.2.28 Log on as a service	<Not Defined>		
4.2.29 Manage auditing and security log	<Not Defined>		Administrators
4.2.30 Modify firmware environment values	<Not Defined>		Administrators
4.2.31 Perform volume maintenance tasks	<Not Defined>		Administrators
4.2.32 Profile single process	<Not Defined>		Administrators
4.2.33 Profile system performance	<Not Defined>		Administrators

Setting:	**Legacy**	**Enterprise**	**Specialized Security – Limited Functionality**
4.2.34 Remove computer from docking station	<Not Defined>		Administrators
4.2.35 Replace a process level token	NETWORK SERVICE, LOCAL SERVICE		
4.2.36 Restore files and directories	<Not Defined>		Administrators
4.2.37 Shut down the system	<Not Defined>	Administrators	
4.2.38 Synchronize directory service data	<None>		
4.2.39 Take ownership of file or other objects	Administrators		
4.3 Other System Requirements			
4.3.1 Ensure volumes are using the NTFS file system	All volumes		
4.3.2 Disable NetBIOS	<Not Defined>		
4.3.3 Enable the Internet Connection Firewall	<Not Defined>		
4.3.4 Restricted Groups	Remote Desktop Users: <None>		
4.3.5 Antivirus software present	<Not Defined>		
4.4 File and Registry Permissions			
4.4.1 File Permissions			
* Unless stated otherwise, Administrators or System Full Control is full control for the designated folder and all contents.			
4.4.1.1 %SystemDrive%	<Not Defined>		Administrators: Full; System: Full; Creator Owner: Full; Interactive: Read, Execute
4.4.1.2 %SystemRoot%\system32\ at.exe	Administrators: Full; System: Full		
4.4.1.3 %SystemRoot%\system32 \attrib.exe	Administrators: Full; System: Full		
4.4.1.4 %SystemRoot%\system32\ cacls.exe	Administrators: Full; System: Full		
4.4.1.5 %SystemRoot%\system32\ debug.exe	Administrators: Full; System: Full		

Setting:	Legacy	Enterprise	Specialized Security – Limited Functionality
4.4.1.6 %SystemRoot%\system32\ drwatson.exe	Administrators: Full; System: Full		
4.4.1.7 %SystemRoot%\system32\ drwtsn32.exe	Administrators: Full; System: Full		

Setting:	**Legacy**	**Enterprise**	**Specialized Security – Limited Functionality**
4.4.1.8 %SystemRoot%\system32\ edlin.exe	Administrators: Full; System: Full; Interactive: Full		
4.4.1.9 %SystemRoot%\system32\ eventcreate.exe	Administrators: Full; System: Full		
4.4.1.10 %SystemRoot%\system32\ eventtriggers.exe	Administrators: Full; System: Full		
4.4.1.11 %SystemRoot%\system32\ ftp.exe	Administrators: Full; System: Full; Interactive: Full		
4.4.1.12 %SystemRoot%\system32\ net.exe	Administrators: Full; System: Full; Interactive: Full		
4.4.1.13 %SystemRoot%\system32\ net1.exe	Administrators: Full; System: Full; Interactive: Full		
4.4.1.14 %SystemRoot%\system32\ netsh.exe	Administrators: Full; System: Full		
4.4.1.15 %SystemRoot%\system32\ rcp.exe	Administrators: Full; System: Full		
4.4.1.16 %SystemRoot%\system32\ reg.exe	Administrators: Full; System: Full		
4.4.1.17 %SystemRoot%\regedit.exe	Administrators: Full; System: Full		
4.4.1.18 %SystemRoot%\system32\ regedt32.exe	Administrators: Full; System: Full		
4.4.1.19 %SystemRoot%\system32\ regsvr32.exe	Administrators: Full; System: Full		
4.4.1.20 %SystemRoot%\system32\ rexec.exe	Administrators: Full; System: Full		
4.4.1.21 %SystemRoot%\system32\ rsh.exe	Administrators: Full; System: Full		
4.4.1.22 %SystemRoot%\system32\ runas.exe	Administrators: Full; System: Full; Interactive: Full		
4.4.1.23 %SystemRoot%\system32\ sc.exe	Administrators: Full; System: Full		

Setting:	Legacy	Enterprise	Specialized Security – Limited Functionality
4.4.1.24 %SystemRoot%\system32\ subst.exe	Administrators: Full; System: Full		
4.4.1.25 %SystemRoot%\system32\ telnet.exe	Administrators: Full; System: Full; Interactive: Full		
4.4.1.26 %SystemRoot%\system32\ tftp.exe	Administrators: Full; System: Full; Interactive: Full		
4.4.1.27 %SystemRoot%\system32\ tlntsvr.exe	Administrators: Full; System: Full		
4.4.2 Registry Permissions			
* Unless stated otherwise, Administrators or System Full Control is full control for the designated key and all subkeys. Creator Owner Full Control is for subkeys only. Users permissions are for current key, subkeys, and values.			
4.4.2.1 HKLM\Software	<Not Defined>		Administrators: Full; System: Full; Creator Owner: Full; Users, Read
4.4.2.2 HKLM\Software\Microsoft\ Windows\CurrentVersion\Installer	Administrators: Full; System: Full; Users: Read		
4.4.2.3 HKLM\Software\Microsoft\ Windows\CurrentVersion\Policies	Administrators: Full; System: Full; Authenticated Users: Read		
4.4.2.4 HKLM\System	<Not Defined>		Administrators: Full; System: Full; Creator Owner: Full; Users, Read
4.4.2.5 HKLM\System\ CurrentControlSet\Enum	Administrators: Full; System: Full; Authenticated Users: Read		
4.4.2.6 HKLM\System\ CurrentControlSet\Services\ SNMP\Parameters\ PermittedManagers	Administrators: Full; System: Full; Creator Owner: Full		

4.4.2.7 HKLM\System\ CurrentControlSet\Services\ SNMP\Parameters\ ValidCommunities	Administrators: Full;
	System: Full;
	Creator Owner: Full		

Setting:	Legacy	Enterprise	Specialized Security – Limited Functionality
4.4.2.8 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Ratings	<Not Defined>		Administrators: Full; Users: Read
4.4.2.9 HKLM\Software\Microsoft\MSDTC	<Not Defined>		Administrators: Full; System: Full; Network Service: Query value, Set value, Create subkey, Enumerate Subkeys, Notify, Read permissions; Users: Read
4.4.2.10 HKU\.Default\Software\Microsoft\SystemCertificates\ Root\ProtectedRoots	Administrators: Full; System: Full; Users: Read		
4.4.2.11 HKLM \SOFTWARE\Microsoft\Windows NT\CurrentVersion\SeCEdit	Administrators: Full; System: Full; Users: Read		
4.4.3 File and Registry Auditing			
4.4.3.1 %SystemDrive%	<Not Defined>		Everyone: Failures
4.4.3.2 HKLM\Software	<Not Defined>		Everyone: Failures
4.4.3.3 HKLM\System	<Not Defined>		Everyone: Failures

Section 2 – Expanded Descriptions of Security Modifications

1 Service Packs and Hotfixes

Microsoft periodically distributes large updates to its operating systems in the form of Service Packs as often as once every few months, or less frequently. Service Packs include all major and minor fixes up to the date of the service pack, and are extensively tested by Microsoft prior to release. In light of the vast number of applications available, it is entirely possible that a bug in a Service Pack may not be discovered, and may slip through this engineering analysis process. Service Packs should be used in a test environment before being pushed into production. If a test system is not available, wait a week or two after the release of a Service Pack, and pay attention to the Microsoft web site for potential bug reports. Additional mailing list and Internet resources are listed in the appendices of this document.

It is important to be aware that Service Packs and Hotfixes are not just applicable to operating systems. Individual applications have their own Service Pack and Hotfix requirements. A Windows system that is completely current on Windows Hotfixes and Service Packs also needs to be kept current with Service Packs and Hotfixes for Internet Explorer and Microsoft Office. The total security of the system requires attention to both operating system and application levels.

Between the releases of Service Packs, Microsoft distributes intermediate updates to their operating systems in the form of Hotfixes. These updates are usually small and address a single problem.

Hotfixes can be released within hours of discovery of any particular bug or vulnerability, because they address a single problem. Since they are normally released so quickly, they do not pass the rigorous testing involved with Service Packs. They should be used with caution at first, even more so than Service Packs. Each Hotfix includes a description of the issue it resolves, whether it is security related, or it fixes a different sort of problem. These should be weighed to determine if the risk of installing the Hotfix is worth the risk of not installing it.

Periodically, Microsoft will release a Hotfix "Roll-up" which is medium ground between a Hotfix and a Service Pack.

1.1 Major Service Pack and Hotfix Requirements

1.1.1 Current Service Pack installed

Description: **<u>WARNING:</u>** Although Service Packs are generally reliable and go through extensive testing, it is <u>possible</u> that it is not compatible with every software product on the market. If possible, test service packs in a test environment, or at least wait until it has been released for a short while before installing it, and watch for industry feedback on the compatibility of that service pack.

At the time of this writing, SP2 has been released for Windows Server 2003.

Recommendation Level: 1

Audit: From the start menu click run and type “winver.exe” in and hit enter. Check that service pack 2 is installed.

Remediation: Install the latest service pack via windows update.

Compliance Mapping: N/A

Additional References: N/A

1.2 Minor Service Pack and Hotfix Requirements

1.2.1 All Critical and Important Hotfixes available to date have been installed.

Description: **WARNING:** Although Hotfixes are generally reliable and go through some testing, it is significantly possible that a Hotfix addressing a single problem is not compatible with every software product on the market, and may cause other problems. If possible, test Hotfixes in a test environment, or at least wait until they have been released for a short while before installation, and watch for industry feedback on the compatibility of those Hotfixes.

Recommendation Level: 1

Audit:

Remediation:

Compliance Mapping: N/A

Additional References: N/A

2 Auditing and Account Policies

Section 2 Audit Preamble:
To execute the following audit and remediation steps first do the following. Start->run, type “mmc.exe”. File->Add/Remove Snap-in and select the “Security Configuration and Analysis” plugin. Hit add and then close the window. You should now have a “Security Configuration and Analysis” item in the list under “Console Root”. Right click on “Security Configuration and Analysis” and go to “Open Database” and type in a new database name. When prompted for an .inf file select security_setup.inf. Back in the main window right click again on “Security Configuration and Analysis” and click “Analyze Computer Now…”.

1. To enable the packet level items in the security options section of the “Security Configuration and Analysis” section replace your %sysroot%\inf with the CIS-provided sceregvl.inf which is part of the appendix.
2. Open a cmd.exe window and type “regsvr32 scecli.dll.”
3. Ensure that regsvr32 successfully registered.

Section 2 Remediation Preamble:
Once you have set the “Database Setting to the value you desire right click on the “Security Configuration and Analysis” list item and click on “Configuration Computer Now” which will use all

of the Database Setting and apply them to the computer as its local policy.

2.1 Major Auditing and Account Policies Requirements

2.1.1 Minimum Password Length

Description: In general, password length and password complexity requirements are used to protect against password guessing attacks. These attacks are relatively unsophisticated: the crack is simply to make repeated guesses to see if the correct password has been chosen. The attack is usually performed in a manner to circumvent account lockout policies. The attempts are typically systematic and can be broken into two categories:

- Dictionary attacks start with a list of common words that may be used to form passwords. The words may be combined, broken down or sent through a variety of "morphing" algorithms to improve effectiveness.
- Brute force attacks walk through all the possible character combinations. First "AAAA1" is tried, then "AAAA2", then "AAAA3", and so on. Once all the five character passwords have been tried, the search begins anew with six character passwords.

In addition to password guessing attacks, some legacy Microsoft protocols suffer from a limitation which makes an eight character password particularly important. These protocols effectively break down passwords into seven character "chunks". This creates two significant vulnerabilities:

- First, passwords with seven or fewer characters are quickly identified.
- Second, since a fourteen character password effectively becomes two seven character passwords, it is actually only twice as secure as a seven character password.

In order to protect against the first vulnerability, the general consensus requires passwords to be eight characters or more.

Protection against the second vulnerability, however, can only be provided through the use of stronger authentication protocols. In particular, LAN Manager (LANMan) and NTLM authentication contains this limitation; however, NTLMv2 and Kerberos are not affected by this. See 3.2.1.52, which discuss how to require NTLMv2 or Kerberos authentication, and how to disable storage of LANMan password hashes.

Recommendation Level: 1

Audit: Expand "Account Policies" and open "Password Policy" and observe the "Minimum password length" setting

Remediation: Set the "Minimum password length" to 10 characters.

2.1.2 Minimum Password Age

Description: All passwords must be changed regularly to ensure passwords they are known only by individuals authorized to use the account.

In addition to limiting user accounts to a single user, this also controls the use of "role" accounts. Role accounts typically may be shared among users for maintenance and troubleshooting, or they may be required for various system services and applications, and are assigned privileges based on their specific purpose. Over time, role account passwords become well-known and an easy route to access resources. Since the accounts are shared by multiple individuals, it becomes very difficult to assign accountability when they are misused. The local administrator and various service accounts are often overlooked, and may have stale passwords which are well known by support personnel.

The requirement to change passwords also provides a practical defense against brute force password attacks. Given the nature of the brute force attack, it will always succeed if there is enough time to eventually guess the password. On a typical computer, it may take weeks or even months to guess a long alphanumeric password. However, if the password expired and has changed during this period, the attack will fail. Therefore the maximum password length is also driven by the capacity of the most common password crack software.

Recommendation Level: 1

Audit: Expand "Account Policies" and open "Password Policy" and observe the "Minimum password length" setting.

Remediation: Expand "Account Policies" and open "Password Policy" and set the "Minimum password length" setting.

2.2 Minor Auditing and Account Policies Requirements

2.2.1 Audit Policy (minimums)

Audit Policy defines the significant events which a computer should log. The log entries, or events, perform two important roles: they provide a means for near-real-time monitoring of the system, and they allow investigation of actions which occurred in the past.

When considering system security, audit events will often identify unauthorized attempts to access resources. The events can be generated from interactive user sessions, or from automated system processes and services.

2.2.1.1 Audit account logon events

Description: Audit logon events to track all attempts to access the computer. These may come from a local interactive logon, a network logon, a batch process, or even a service. Failed account logons may show a trend for password attacks; successful logon events are important to identify which user was logged on to the computer at a given time. “Account Logon” events are generated from the use of domain accounts; this differs from “Logon Events” (2.2.1.4) which are generated by the use of local accounts.

Recommendation Level: 1

Audit: Expand “local policies” then “Audit Policy” and view “Audit account logon events”.

Remediation: Set “Audit account logon events” to log during Success or Failure.

Additional References:
http://technet2.microsoft.com/windowsserver/en/library/e104c96f-e243-41c5-aaea-d046555a079d1033.mspx?mfr=true

2.2.1.2 Audit account management

Description: In order to track successful and failed attempts to create new users or groups, rename users or groups, enable or disable users, or change accounts’ passwords, enable auditing for Account Management events. Successful account management events are also generated when an account is locked out, so these events become important in determining the cause of an account lockout.

Recommendation Level: 1

Audit: Expand “local policies” then “Audit Policy” and view “Audit account management”.

Remediation: Expand “local policies” then “Audit Policy” and view “Audit account management” and ensure the “Computer Setting” is set to “Success, Failure”.

2.2.1.3 Audit directory service access

Description: Enable directory service access auditing to track access to objects within Active Directory. This requires specific objects to have system access control lists configured for auditing. Enabling directory service access auditing may generate a large amount of log entries, and must be implemented with care.

Recommendation Level: 1

Audit: Expand “local policies” then “Audit Policy” and view “Audit Directory Service Access”.

Remediation: Expand “local policies” then “Audit Policy” and view “Audit Directory Service Access” and set the “Database Setting” to “Success, Failure”.

2.2.1.4 Audit logon events

Description: Similar to 2.2.1.1 above, Logon Events will identify which accounts are accessing resources on the local computer. These events are generated only when local machine credentials are used. Even if a machine is domain member, it is still possible to log on to the computer using a local account.

Recommendation Level: 1

Audit: Expand “local policies” then “Audit Policy” and view “Audit logon events”.

Remediation: Expand “local policies” then “Audit Policy” and set “Audit logon events” to “Success, Failure”.

2.2.1.5 Audit object access

Description: It is possible to track when specific users access specific files. This option only produces events when one or more objects are actively being audited.

In order to track user access to specific files or directories, navigate to the file or folder, edit the security properties for that object, and enable auditing on the object.

Caution: *Enabling this setting may generate an excessive amount of log entries depending on the number of objects that have auditing enabled.*

Recommendation Level: 1

Audit: Expand “local policies” then “Audit Policy” and view “Audit object access”.

Remediation: Expand “local policies” then “Audit Policy” and set the “Database Setting” of “Audit object access” to “Success, Failure”.

2.2.1.6 Audit policy change

Description: When the “Audit Policy Change” option is set, changes to User Rights, Audit Policies, or Trust Policies will produce events in the Security Event Log.

Recommendation Level: 1

Audit: Expand “local policies” then “Audit Policy” and view “Audit policy change”.

Remediation: Expand “local policies” then “Audit Policy” and set the “Database Setting” of “Audit policy change” to “Success, Failure”.

2.2.1.7 Audit privilege use

Description: Auditing privilege use enables auditing for any operation that would require a user account to make use of extra privileges that it has already been assigned. If this is enabled, events will be generated in the security event log when a user or process attempts to bypass traverse checking, debug programs, create a token object, replace a process level token, or generate security audits.

If security credentials are used to backup or restore files or directories using the “Backup or Restore” user right, and if this setting is set, security events will be generated.

Privilege Use is used by all user accounts on a regular basis. If success and failure events are audited, there will be a great many events in the event log reflecting such use.

Caution: *Enabling this setting may generate an excessive amount of log entries.*

Recommendation Level: 1

Audit: Expand “local policies” then “Audit Policy” and view “Audit privilege use”.

Remediation: Expand “local policies” then “Audit Policy” and set the “Database Setting” of “Audit privilege use” to “Failure”.

2.2.1.8 Audit process tracking

Description: When this option is enabled, an event is generated each time an application or a user starts, stops, or otherwise changes a process. This creates a very large event log very quickly, and the information is not normally exceptionally useful, unless you are tracking a very specific behavior. Auditing process tracking is not required, and is only recommended when absolutely necessary.

Caution: *Enabling this setting may generate an excessive amount of log entries.*

Recommendation Level: 1

Audit: Expand “local policies” then “Audit Policy” and view “Audit process tracking”.

Remediation: Expand “local policies” then “Audit Policy” and set the “Database Setting” of “Audit process tracking” to “Failure”.

2.2.1.9 Audit system events

Description: Auditing System events is very important. System events include starting or shutting down the computer, full event logs, and other items which impact the computer, but may not be directly related to security. System events are particularly useful when reviewing a system during or after an incident. Auditing of Success events should be enabled. Microsoft insists that there are no “failed” system events, so auditing them has no effect.

Recommendation Level: 1

Audit: Expand “local policies” then “Audit Policy” and view “Audit system events”.

Remediation: Expand “local policies” then “Audit Policy” and set the “Database Setting” of “Audit system events” to “Failure”.

2.2.2 Account Policy

When applying the account settings below (password, lockout and Kerberos policies), it is important to consider exactly where these settings must be applied to affect different account types:

- If the computer is not a member of a domain, these policies can be applied locally and will be consistently applied to all local accounts.
- If the computer belongs to a domain, any settings applied here will not impact domain accounts. Account policy for domain accounts can only specified in the domain policy.
- If the computer belongs to an Active Directory domain, and is placed in a specific Organizational Unit (OU), account policy can be placed on that OU. The OU policy will apply to all local accounts on the computer, and will override the local security policy. The same holds true for other Active Directory containers such as Sites and entire domains.

See Microsoft Knowledge Base Article 255550 for more information.

2.2.2.1 Minimum password age

Description: The recommended password policy requires users to change passwords regularly, and requires the password to be different from those cached in history. When the minimum password age is set to 0, a user can change passwords repeatedly. It is possible for the user to continue changing passwords until yesterday’s password is flushed from the cache, and then re-use the old password. This activity is prevented by limiting password changes to once a day.

Maximum and minimum password age requirements are enforced by the logon process. If an account never logs off, it will continue to gain access to resources until the system reboots or forces that user to re-authenticate.

Recommendation Level: 1

Audit: Expand “Security Configuration and Analysis in the Console Root of the Microsoft Management Console. Then expand “Account Policies” and click on “Password Policy”. Now view the “Minimum Password Age” setting.

Remediation: Expand “Security Configuration and Analysis in the Console Root of the Microsoft Management Console. Then expand “Account Policies” and click on “Password Policy”. Now set the “Minimum Password Age” to “0 days”.

2.2.2.2 Maximum password age

Description: All passwords must be changed regularly to ensure passwords they are known only by individuals authorized to use the account.

In addition to limiting user accounts to a single user, this also controls the use of “role” accounts. Role accounts typically may be shared among users for maintenance and troubleshooting, or they may be required for various system services and applications, and are assigned privileges based on their specific purpose. Over time, role account passwords become well-known and an easy route to access resources. Since the accounts are shared by multiple individuals, it becomes very difficult to assign accountability when they are misused. The local administrator and various service accounts are often overlooked, and may have stale passwords which are well known by support personnel.

The requirement to change passwords also provides a practical defense against brute force password attacks. Given the nature of the brute force attack, it will always succeed if there is enough time to eventually guess the password. On a typical computer, it may take weeks or even months to guess a long alphanumeric password. However, if the password expired and was changed since the attack began, it will discover a password that has already been changed. Therefore the maximum password length is also driven by the capacity of the most common password attack/audit software.

Recommendation Level: 1

Audit: Expand “Security Configuration and Analysis in the Console Root of the Microsoft Management Console. Then expand “Account Policies” and click on “Password Policy”. Now view the “Maximum Password Age” setting.

Remediation: Expand “Security Configuration and Analysis in the Console Root of the Microsoft Management Console. Then expand “Account Policies” and click on “Password Policy”. Now set the “Maximum Password Age” setting to “15 days”.

2.2.2.3 Minimum password length

Description: Password length significantly increases resistance to brute force attacks. A single extra character makes a large difference: even if passwords are case insensitive and alphanumeric, one extra password means the typical brute force attack will take 36 times as long (10 digits plus 26 letters) to complete.

Recommendation Level: 1

Audit: Expand “Security Configuration and Analysis in the Console Root of the Microsoft Management Console. Then expand “Account Policies” and click on “Password Policy”. Now view the “Minimum Password Length” setting.

Remediation: Expand “Security Configuration and Analysis in the Console Root of the Microsoft Management Console. Then expand “Account Policies” and click on “Password Policy”. Now set the “Minimum Password Length” setting in the “Database setting” column to “10”.

2.2.2.4 Password complexity

Description: Section 2.1.1 introduced the brute force password attack. Complex passwords further mitigate the risk of a brute force password attack by significantly increasing the set of all possible passwords. This is done by requiring passwords to include a combination of upper and lowercase letters, numbers and symbols (special characters) in the password.

Windows 2003 does not provide any granularity in password complexity requirements—it is either on or off. When complex passwords are required, each password must contain characters from three of the following four sets of characters:

- Uppercase letters
- Lowercase letters
- Numbers
- Special characters (non alphanumeric symbols)

Enabling this setting provides substantial resistance to brute force password attacks, and should be set whenever possible, but may occasionally be difficult to implement. End-user education is a must, as the warning messages for weak passwords are cryptic and likely to be of little help to most users. Also, consider the impact to other non-Microsoft systems which integrate with the Microsoft authentication scheme, and make sure they support complex passwords as well.

If you are unable to require complex passwords, consider lengthening the minimum password length. Often a long alphabetic passphrase can be more resistant to a brute force attack than a short complex passphrase.

Recommendation Level: 1

Audit: Expand “Security Configuration and Analysis” in the Console Root of the Microsoft Management Console. Then expand “Account Policies” and click on “Password Policy”. Now view the “Password must meet complexity requirements” setting.

Remediation: Expand “Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand “Account Policies” and click on “Password Policy”. Now set the “Password must meet complexity requirements” setting in the “Database setting” column to “Enabled”.

2.2.2.5 Password History

Description: Passwords should be changed on a regular basis. By that same rule, users should not be permitted to use the same few passwords over and over again. The Enforce Password History setting determines how many previous passwords are stored to ensure that users do NOT cycle through regular passwords. The NSA requirement of 24 passwords remembered should be viable for public use as well.

When determining your overall account configuration, consider the combined effect of password history and maximum password age settings, and prevent repetitive patterns. For example, if your password age is 30 days and password history is 12 or less, many users will likely to set passwords to a variation of the current month (January1, February1, etc.).

Recommendation Level: 1

Audit: Expand “Security Configuration and Analysis” in the Console Root of the Microsoft Management Console. Then expand “Account Policies” and click on “Password Policy”. Now view the “Enforce Password History” setting.

Remediation: Expand “Security Configuration and Analysis” in the Console Root of the Microsoft Management Console. Then expand “Account Policies” and click on “Password Policy”. Now set the “Enforce Password History” setting in the “Database Setting” column to “24 passwords remembered”.

2.2.2.6 Store password using reversible encryption

Description: The Windows authentication model allows storage of a password hash rather than the actual password. A password hash can not be decoded to regain the original password. Rather, to authenticate, the password must be hashed exactly the same way and compared with the original stored hash. If the values match, the correct password was presented, and access is granted.

In order to support some applications and their authentication, Microsoft permits the ability to store passwords using reversible encryption. If at all possible, this should be avoided. This option is disabled by default, and should remain so. Any application that requires reversible encryption for passwords is purposely putting systems at risk.

Recommendation Level: 1

Audit: Expand “Security Configuration and Analysis” in the Console Root of the Microsoft Management Console. Then expand “Account Policies” and click on “Password Policy”. Now view the “Store passwords using reversible encryption” setting.

Remediation: Expand “Security Configuration and Analysis” in the Console Root of the Microsoft Management Console. Then expand “Account Policies” and click on “Password Policy”. Now set the “Store passwords using reversible encryption” setting in the “Database Setting” column to “Disabled”.

2.2.3 Account Lockout Policy

Many of the settings above protect against brute force and dictionary password attacks. Typically these attacks gather information (such as password hashes) and perform the attack offline. However, some password guessing attacks still occur interactively.

2.2.3.1 Account lockout duration

Description: Once the criteria for a lockout are met, the account becomes locked. However, the account will automatically become re-enabled once again after the duration specified in the “Account Lockout Duration.” Specify 0 minutes to have the account remain locked out until an administrator manually unlocks the account.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Account Policies" and click on "Account Lockout Policy". Now view the "Account Lockout Duration" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Account Policies" and click on "Account Lockout Policy". Now set the "Account Lockout Duration" setting in the "Database Setting" column to "24 hours".

2.2.3.2 Account lockout threshold

Description: The user is given a number of attempts to enter the wrong password before their account becomes locked. The “Account Lockout Threshold” defines this limit.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Account Policies" and click on "Account Lockout Policy". Now view the "Account Lockout Threshold" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Account Policies" and click on "Account Lockout Policy". Now set the "Account Lockout Threshold" setting in the “Database Setting” column to “3 invalid logon attempts”.

2.2.3.3 Reset account lockout counter after

Description: Following a bad logon, the system increments the count of invalid attempts for this account. This counter continues to increment until the lockout threshold is reached, or the counter is reset. The “Reset Account Lockout After” setting defines how often the counter is reset. This setting must be less than or equal to the “Account Lockout Duration”, 2.2.3.1.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Account Policies" and click on "Account Lockout Policy". Now view the "Reset account lockout counter after" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Account Policies" and click on "Account Lockout Policy". Now set the "Reset account lockout counter after" setting in the “Database Setting” column to “1 hour”.

2.2.4 Event Log Settings

All system events are collected into event logs. All Windows systems contain three sets of logs: Application, System and Security. Application logs entries typically come from installed software; for example, anti-virus software will create an event when virus scans complete, or when it detects a virus. The System log collects events generated by the operating system, such as system reboots and a startup or shutdown of event logs.   The security log collects security audit information as defined by the audit policy. All three logs may contain useful information about a security incident.

The default size of each event log is 512k. This has been standard since the days of Windows NT 3.5, when hard drives were typically less than 2 Gigabytes (GB) in size. However, recent hardware capacity improvements should leave ample storage space for an 80Mb event log.

Two additional settings control system behavior when the event log is full. Essentially there are two possibilities:

- Continue logging events as they come but risk overwriting important events
- Stop logging events

Obviously, it is preferable to continue logging events so that useful information is not lost. However, consider the attacker that kicks off a fake event generator as the last step of the attack (for example, it might try to log in with the guest account hundreds of times a second knowing the guest account is disabled). If all events continue to be logged, the events from the actual attack will soon be overwritten. In this case, it would be preferable to stop logging events when the log fills.

The Audit policy setting for "Log Retention Method" provides control over how the system reacts to a full log:

- **Overwrite Events as Needed** continues logging all events, overwriting older event whenever necessary.
- **Overwrite by Days**, allows overwriting some events, but not all. Events older that a specific number of days can be cleared out. Once all the older events are overwritten, no new events are logged.
- **Do not overwrite (Clear logs manually)** prevents overwriting events, and new events are lost when the event log fills. The event log must be cleared manually by the system administrator or an automated log management application.

Given that the allowed value for event log size can be up to 4Gb, it may seem reasonable to put a higher limit on the total event log size than that listed below. However, the event logs must be maintained in contiguous memory due to the application design. On current systems, it would be rare to find a block of contiguous memory larger than 240Mb, and the actual log size would be limited to the amount available. For additional details about this limit, see the "Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP" (available for download from the Microsoft web site, http://www.microsoft.com/2003), chapter 6, "Maximum event log size". The settings below reflect a reasonable weighting for the different log types.

Setting the "Log Retention Method" to "Overwrite by Days" enables the "Log Retention" option. This specifies the number of days of event logs the system will preserve.

3 Security Settings

Security settings outline many very specific options which can improve a system's security by protecting against a specific threat.

To edit security settings, select Start | Settings | Control Panel. Double-click "Administrative Tools," and select "Local Security Policy". In the window that appears, expand Local Policies, and click Security Options. To make changes, double-click one of the settings in the right pane, make the appropriate changes, and click OK to save the settings.

If the workstation is not a member of a domain, the change will become effective immediately, even though it won't show up in the Local Security Policy editor until it is closed. If the workstation belongs to a domain, local changes will only become effective domain policy does not override the settings.

3.1 Major Security Settings

Microsoft operating systems typically support a legacy anonymous login known as a "null session". The null session is actually a login session where both the user id and the password are blank. Although the operating system places many restrictions on a null session, and it can never be used for an interactive logon, it may still be possible to gather significant information through this special anonymous account.

Null sessions can usually be safely disabled since they are a legacy feature. However, some legacy applications may cease to function properly after disabling null sessions, so testing is a must. The settings below outline controls available within Windows 2003 to limit exactly what information can be obtained through the null session. Note that these settings affect local workstation accounts and resources only, but not domain accounts and shares.

Note that Windows 2000 manages this setting differently, although the net effect remains the same. In Windows 2000, these options correspond to “Additional Restrictions for Anonymous Connections.” Other minor differences in Windows 2000 and Windows 2003 policies as well, and Windows 2000 tools should not be used when setting policy for Windows 2003 machines.

3.1.1 Network Access: Allow anonymous SID/Name translation

Description: Each object within Active Directory obtains a unique binary security identifier (SID). The operating system controls access to resources by their SID. SID formatting is well known, and some SIDs (e.g., local administrator and local guest) have properties which divulge the actual purpose of the account.

Disable this option to prevent the null user from translating the binary SID into the actual account name.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Network access: Allow anonymous SID/Name translation" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Network access: Allow anonymous SID/Name translation" setting in the “Database Setting” column to “disabled”.

3.1.2 Network Access: Do not allow anonymous enumeration of SAM accounts

Description: By default, the null session login can list all the accounts within its domain. This presents a significant security risk, particularly if strong passwords are not required. Should an attacker be able to anonymously gather all available accounts, they can then try some basic guessing to quickly locate accounts with blank or very weak passwords.

SAM stands for the Security Account Manager. The SAM database holds all account information including passwords, access rights and special privileges. Local account information resides in the local SAM database, a file on the workstation. Domain account information resides in the SAM database on the domain controller.

Beware of the syntax for this option: Enabled means only truly authenticated logins may enumerate other accounts; Disabled means all accounts can be gathered through the null session.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Network access: Do not allow anonymous enumeration of SAM accounts" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Network access: Do not allow anonymous enumeration of SAM accounts" setting in the “Database Setting” column to “enabled”.

3.1.3 Network Access: Do not allow anonymous enumeration of SAM accounts and shares

Description: In addition to protecting the list of user accounts, it also controls the list of network file shares established on the workstation. Documentation does not describe behavior if this setting conflicts with 3.1.1; however, if this setting is enabled, 3.1.1 should be enabled as well.

Beware of the syntax for this option: Enabled means only truly authenticated logins may enumerate accounts and shares; Disabled means all accounts and file shares can be gathered through the null session.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Network access: Do not allow anonymous enumeration of SAM accounts and shares" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Network access: Do not allow anonymous enumeration of SAM accounts and shares" setting in the “Database Setting” column to “Enabled”.

3.2 Minor Security Settings

3.2.1 Security Options

Security settings outline many very specific options which can improve a system’s security by protecting against a specific threat.

To edit security settings, select Start | Settings | Control Panel. Double-click “Administrative Tools,” and select “Local Security Policy”. In the window that appears, expand Local Policies, and click Security Options. To make changes, double-click one of the settings in the right pane, make the appropriate changes, and click OK to save the settings.

If the workstation is not a member of a domain, the change will become effective immediately, even though it won’t show up in the Local Security Policy editor until it is closed. If the workstation belongs to a domain, local changes will only become effective domain policy does not override the settings.

3.2.1.1 Accounts: Administrator account status

Description: Each Windows installation creates an “Administrator” account which has the highest access to the system. The account has highest level access and can bypass most security controls local to the machine; it is comparable to the “root” account in Unix. Many system maintenance features require use of the Administrator account.

However, in some environments, the existence of this account can present a security risk. By setting the “Administrator Account Status” to disabled, the account becomes unavailable.

Regardless of this setting, the administrator account remains enabled when booting in “safe mode.”

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Accounts: Administrator account status" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Accounts: Administrator account status" setting in the “Database Setting” column to disabled.

3.2.1.2 Accounts: Guest account status

Description: The Guest account can provide some regulation to unauthenticated users. Disabling this account will prevent unknown users being authenticated as Guests. This default installation disables this account, and it should remain disabled. is disabled by default, and should remain so.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Accounts: Guest account status" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Accounts: Guest account status" setting in the “Database Setting” column to disabled.

3.2.1.3 Accounts: Limit local account use of blank passwords to console logon only

Description: Windows divides computer logons into two main types: console or local logons and remote logons. In a console logon, the user physically logs on to the device with the attached keyboard. Remote logons are performed across the network using various protocols such as RPC, telnet, FTP and remote desktop.

When this setting is enabled, the computer refuses remote logons if the user attempts to use a blank password, even if the blank password is valid for that account. This setting should be enabled even though passwords should never be left blank.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Accounts: Guest account status" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security

Options". Now set the "Accounts: Guest account status" setting in the "Database Setting" column to "Enabled".

3.2.1.4 Accounts: Rename administrator account

Description: See 3.2.1.1. Often disabling the Administrator account is not practical. However, simply knowing the name of an account on a machine can be valuable information to an attacker. In an attempt to hide the account, best practices recommend renaming the account to something unique for your implementation.

If the account is renamed, anonymous Security Identifier (SID) / Name translation should also be disabled (3.1.1). This prevents an attacker from locating the renamed account by its SID.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "Accounts: Rename administrator account" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "Accounts: Rename administrator account" setting in the "Database Setting" column to "InNoWayTheAdminAccount".

3.2.1.5 Accounts: Rename guest account

Description: See 3.2.1.2. Similar to the Administrator account, the Guest account should be renamed even if it is disabled. The operating system places additional safeguards on the Guest account, and it is less of a target than the Administrator account, but it still deserves significant attention warrant changing the account name.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "Accounts: Rename guest account" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "Accounts: Rename guest account" setting in the "Database Setting" column to "NotTheGuestAccount".

3.2.1.6 Audit: Audit the access of global system objects

Description: Global system objects typically only provide interesting audit information to developers. Some examples of these kernel objects include mutexes, semaphores and DOS devices. Normal system operation does not require auditing to this level of detail.

"Audit Object Access (2.2.1.5)" must be enabled before this setting will generate log entries.

Caution: *Enabling this setting may generate an excessive amount of log entries.*

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Audit: Audit the access of global system objects" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Audit: Audit the access of global system objects" setting in the “Database Setting” column to “Enabled”.

3.2.1.7 Audit: Audit the use of Backup and Restore privilege

Description: When enabled, this setting will generate a log entry for every object which is backed up or restored using the “Backup or Restore” user right. During normal operations, this will generate a large amount of event entries, and is typically not required just stay on top of what users have backup and restore rights and restrict it to only necessary users.

“Audit Privilege Use (2.2.1.7)” must be enabled before this setting will generate log entries.

Caution: *Enabling this setting may generate an excessive amount of log entries.*

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Audit: Audit the use of Backup and Restore Privilege" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Audit: Audit the use of Backup and Restore Privilege" setting in the “Database Setting” column to “Enabled”.

3.2.1.8 Audit: Shut down system immediately if unable to log security audits

Description: See Event Log Settings 2.2.4. A system administrator may choose not to overwrite events when the event log is full. Assuming that logs are sized appropriately, routinely backed up and cleared, this could indicate a security incident. In the specialized security environment, the inability to log events may be just cause to halt the server.

If the server is unable to log events and this setting is enabled, a “STOP: C0000244 {Audit Failed}” error occurs. To recover, a member of the Administrators group must log on to the computer and manually clear the event log or change this setting. This enables the administrator to archive the log entries for analysis to see why the log was full.

Security Log Retention Method must be set to “Do Not Overwrite Events” or “Overwrite Events by Days” for this setting to be effective.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security

Options”. Now view the "Audit: shut down system immediately if unable to log security audits" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Audit: shut down system immediately if unable to log security audits" setting in the “Database Setting” column to “Enabled”.

3.2.1.9 Devices: Allow undock without having to log on

Description: Can’t a laptop always be undocked simply by lifting it off the dock? Surprisingly, the answer is no. Some laptop docking stations have a hardware eject button that can actually be locked by software on the laptop. Setting this option to disabled provides greater security; however, without proper training a user may physically damage the hardware. This setting has no effect unless the server is running on a laptop.

Beware of the syntax for this option: Disabled means a user must log in to the laptop and request to undock it; Enabled means the laptop can be unlocked at any time

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Devices: Allow undock without having to log on " setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Devices: Allow undock without having to log on" setting in the “Database Setting” column to “Disabled”.

3.2.1.10 DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax.

Description: This setting determines which users or groups can access DCOM applications remotely or locally. Use this to limit attack surface by only setting the minimum set of users run DCOM applications.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax " setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the " DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax " setting in the “Database Setting” column to the “Distributed COM Users” group.

3.2.1.11 DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax.

Description: This setting determines which users or groups can launch DCOM applications remotely or locally. Use this to limit attack surface by only setting the minimum set of users run DCOM applications.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax " setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the " DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax " setting in the “Database Setting” column to the “Distributed COM Users” group.

3.2.1.12 Devices: Allowed to format and eject removable media

Description: This setting governs the type of users which have authority to remove NTFS formatted media from the computer. The available choices (listed from most to least restrictive) are Administrators, Administrators and Power Users, or Administrators and Interactive Users.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Devices: Allowed to format and eject removable media” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Devices: Allowed to format and eject removable media” setting in the “Database Setting” column to “Administrators”.

3.2.1.13 Devices: Prevent users from installing printer drivers

Description: Users typically need the ability to install and configure their own printers. However, printer driver installation loads code directly into the privileged space of the operating system kernel. The malicious user could choose to install an invalid or Trojan Horse (think back to Troy) print driver to gain control on the system.

Preventing users from installing printer drivers may lead to unwanted support calls. If users must be given the right to install printer drivers, consider requiring that the driver be digitally signed before it can be installed (see 3.2.1.16).

Beware of the syntax for this option: Enabled means the users will not be able to install printer drivers and may prevent proper setup of printers; Disabled allows the user to fully manage their own printers.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Devices: Prevent users from installing printer drivers” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Devices: Prevent users from installing printer drivers” setting in the “Database Setting” column to “Enabled”.

3.2.1.14 Devices: Restrict CD-ROM access to locally logged-on user only

Description: With sufficient privileges, users can create network shares from any folder on a Windows 2003 computer. This extends to sharing a CD-ROM drive externally. This setting would restrict use of the shared CD-ROM drive to the local interactive logon. Since different CDs can be inserted, the user may forget or be unaware that the information on the CD becomes remotely accessible. Also, unlike typical file shares, access control lists can not be placed on files and directories to control access and auditing.

Generally, users and processes should not need to remotely access a workstation CD-ROM drive; however, enabling this setting could cause problems with some software installation packages. When users install software from a CD-ROM drive, and the installation package uses the Microsoft Installer (.msi packages), the Windows Installer service actually performs the installation. The install will fail, since the service account is not actually the locally logged-on user. If this setting is enabled, such software installation will not be able to proceed, because of this restriction. The setting must be changed long enough to install the software, or the package must be copied to a local or network drive for the installation procedure to succeed.

Beware of the syntax for this option: <u>Enabled</u> means users will **not** be able to access CD-ROM shares. <u>Disabled</u> allows access to shared CD-ROMs (share-level access permissions still apply).

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Devices: Restrict CD-ROM access to locally logged-on user only” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Devices: Restrict CD-ROM access to locally logged-on user only” setting in the “Database Setting” column to “Enabled”.

3.2.1.15 Devices: Restrict floppy access to locally logged-on user only

Description: Similar to a CD-ROM drive (3.2.1.14 above), the floppy drive can be shared to network users. Again, the user may not remember that the information on all inserted floppies becomes exposed.

Beware of the syntax for this option: <u>Enabled</u> means users will **not** be able to access shared floppy drives. <u>Disabled</u> allows access to shared floppy drives, but share-level access permissions still apply.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Devices: Restrict floppy access to locally logged-on user only” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Devices: Restrict floppy access to locally logged-on user only” setting in the “Database Setting” column to “Enabled”.

3.2.1.16 Devices: Unsigned driver installation behavior

Description: Drivers interact with the kernel and hardware at a low level; improper drivers can open the system to low level hardware and kernel problems. Additionally, trojaned drivers can open the system to compromise. Microsoft generally ships drivers with a digital signature, expressing that Microsoft itself has certified the drivers through their Windows Hardware Quality Lab. Unfortunately, not all drivers (even from Microsoft) have digital signatures.

Options for this setting are “Silently succeed,” “Warn but allow installation,” and “Do not allow installation.” The user should be notified if drivers are not signed; however, some end-user training may be required. The “Silently succeed” option may be required in managed environments where unattended software installations are commonplace.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Devices: Unsigned driver installation behavior” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Devices: Unsigned driver installation behavior” setting in the “Database Setting” column to “Do not allow installation”.

3.2.1.17 Domain controller: Allow server operators to schedule tasks

Description: When enabled, server operators can add tasks using the AT command. By default, AT runs under the local system account, which has administrative rights on the machine. When this setting is disabled, server operators can still schedule tasks with the task scheduler; however, these tasks will run under their domain credentials and not under the local system account.

This setting has no effect on computers other than Domain Controllers.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Domain controller: Allow server operators to schedule tasks” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Domain controller: Allow server operators to schedule tasks” setting in the “Database Setting” column to “Disabled”.

3.2.1.18 Domain controller: LDAP server signing requirements

Description: This option can be set to Require Signature, None (signing is not required unless the client requests it). Data signing helps protect against man-in-the-middle attacks, but does not protect the confidentiality of data in transit. LDAP signing requires Windows 2003, Windows XP, or Windows 2000 Service Pack 3.

This setting has no effect on computers other than Domain Controllers.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Domain controller: LDAP server signing requirements” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Domain controller: LDAP server signing requirements” setting in the “Database Setting” column to “Disabled”.

3.2.1.19 Domain controller: Refuse machine account password changes

Description: This setting will allow the domain to prevent the computer from changing the computer account password.

This setting has no effect on computers other than Domain Controllers.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Domain controller: Refuse machine account password changes” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Domain controller: Refuse machine account password changes” setting in the “Database Setting” column to “Disabled”.

3.2.1.20 Domain member: Digitally encrypt or sign secure channel data (always)

Description: When a domain member workstation or server boots up, it creates an encrypted tunnel with a domain controller to pass sensitive information. For example, management of the workstation’s computer account password, user account password changes, and the exchange of private keys with Active Directory all occur through this NetLogon secure RPC channel.

With this setting enabled, all packets sent from the client will be signed. The client will also encrypt the packets if the server supports it. A signed packet can not be spoofed or tampered; however, the payload remains untouched and could possibly be deciphered should it be intercepted. Encrypted packets can only be decrypted by the server.

This setting can only be safely enabled when all domain controllers are Windows 2000, or Windows NT SP 4 or later.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Domain member: Digitally encrypt or sign secure channel data (always)” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Domain member: Digitally encrypt or sign secure channel data (always)” setting in the “Database Setting” column to “Enabled”.

3.2.1.21 Domain member: Digitally encrypt secure channel data (when possible)

Description: See 3.2.1.20 above. This setting provides greater compatibility than requiring encryption or signing.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Domain member: Digitally encrypt or sign secure channel data (when possible)” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Domain member: Digitally encrypt or sign secure channel data (when possible)” setting in the “Database Setting” column to “Enabled”.

3.2.1.22 Domain member: Digitally sign secure channel data (when possible)

Description: See 3.2.1.20 above. This setting also provides compatibility with legacy peers. It prevents replay and man-in-the middle attacks when domain controllers support signing. However, by itself, this setting will not protect against packet sniffing to gather potentially sensitive information.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Domain member: Digitally sign secure channel data (when possible)” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Domain member: Digitally sign secure channel data (when possible)” setting in the “Database Setting” column to “Enabled”.

3.2.1.23 Domain member: Disable machine account password changes

Description: If a computer is a member of a domain, it has an account within the domain. During the boot up process, the computer logs in to the domain and establishes a secure channel for the exchange of sensitive information (see 3.2.1.20). Although the account can not be used for interactive logons, it can be used to authenticate to domain resources. This setting only impacts workstations which have joined a domain.

Like any other account, the computer account has a name and password. The computer manages its own password and changes it to a strong password regularly. This setting can be used to prevent the machine from managing its own password. Should the machine's local copy of the password falls out of synch with the domain controller's copy, the machine can not access domain resources, and the machine must be re-joined to the domain.

Beware of the syntax for this option: Disabled means the workstation will change its password; Enabled means workstation passwords are never changed.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "Domain member: Disable machine account password changes" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "Domain member: Disable machine account password changes" setting in the "Database Setting" column to "Enabled".

3.2.1.24 Domain member: Maximum machine account password age

Description: See 3.2.1.23 above. This setting determines how often the computer resets its password. Remember that machine password changes do not visibly impact the end user, and they should be consistent with corporate policy for account management

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "Domain member: Maximum machine account password age" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "Domain member: Maximum machine account password age" setting in the "Database Setting" column to "15 days".

.

3.2.1.25 Domain member: Require strong (Windows 2000 or later) session key

Description: This setting applies specifically to the netlogon secure channel established between workstations and domain controllers (see 3.2.1.20). This setting only impacts workstations which have joined a domain.

By default, workstations will accept a weak 64-bit session key to encrypt the secure channel. However, this setting allows the workstation to require a strong 128-bit session key for the secure channel.

Only enable this setting if all domain controllers support a 128-bit encrypted secure channel. This is not supported on NT4 domain controllers; Windows 2000 domain controllers require Service Pack 2 or later.

This option is enabled by default, and it should remain so.

Recommendation Level: 1

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Domain member: Require strong (Windows 2000 or later) session key” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Domain member: Require strong (Windows 2000 or later) session key” setting in the “Database Setting” column to “Enabled”.

3.2.1.26 Interactive logon: Do not display last user name

Description: Anyone attempting to log into a computer may see the name of the last valid user who logged on to that system. This does not prevent displaying the currently logged on user when unlocking a workstation. This information may seem trivial, but it helps an attacker tie a workstation to a particular individual, or may help an attacker gain access to a stolen mobile device.

Educate users before enabling this setting in a domain environment. Some users may not know their logon, particularly when it differs from the e-mail address or other accounts.

Beware of the syntax for this option: Enabled means the user must type in their user id on every logon; Disabled means the last logged on user appears in the login dialog.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Interactive logon: Do not display last user name” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Interactive logon: Do not display last user name” setting in the “Database Setting” column to “Enabled”.

3.2.1.27 Interactive logon: Do not require CTRL+ALT+DEL

Description: The Windows operating system treats the CTRL+ALT+Delete key sequence different from any other. Operating system design prevents any application from intercepting and responding when these keys are pressed. When you type

CTRL+ALT+Delete, you are guaranteed that the operating system authentication process will handle the request.

With the CTRL+ALT+Delete requirement lifted, the user could actually be typing their password into a trojaned application, rather than the operating system authentication process. Remember, the trojaned application would not be able to respond had the user pressed CTRL+ALT+Delete.

When the console does not require CTRL+ALT+Delete to log on, users will not see the dialog “Press CTRL+ALT+Delete to Log On.” Rather, the workstation simply presents the standard logon dialog.

Beware of the syntax for this option: Disabled means the user must press CTRL+ALT+Delete before every non-smartcard logon; Enabled will present the logon dialog without requiring CTRL+ALT+Delete.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Interactive logon: Do not require CTRL+ALT+DEL” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Interactive logon: Do not require CTRL+ALT+DEL” setting in the “Database Setting” column to “Disabled”.

3.2.1.28 Interactive logon: Message text for users attempting to log on

Description: In general, legal requirements dictate that users must be notified of security practices when logging on to a system. The users should agree to acceptable usage policies, and be notified that the system may be monitored. The message is commonly referred to as a “logon banner”.

The sample banner provided below has been approved by the United States Department of Justice. The United States government deems it suitable for use. For corporate networks and workstations, defer the actual text to your legal counsel, perhaps using this message as a template.

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Interactive logon: Message text for users attempting to log on” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Interactive logon: Message text for users attempting to log on” setting in the “Database Setting” column to an appropriate text as discussed in the description of this item perhaps using the following:

“<u>This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.”</u>

3.2.1.29 Interactive logon: Message title for users attempting to log on

Description: The message title acts as part of the logon banner discussed above. The workstation places this text as the title for the logon banner window. The text should be either neutral or a warning. Avoid inviting titles such as “Welcome”.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Interactive logon: Message title for users attempting to log on” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Interactive logon: Message title for users attempting to log on” setting in the “Database Setting” column to something like “Computer logon (authorized users only)”.

3.2.1.30 Interactive logon: Number of previous logons to cache (in case domain controller is not available)

Description: When a workstation belongs to a domain, users can log on to it using domain credentials. The domain credentials can be cached in the local workstation’s Security Accounts Manager (SAM) database. On next logon, should no domain controller be available, the user can still log on locally by authenticating against the cached account information.

When logging on using cached credentials, some account properties will not be enforced, since the domain controller maintains responsibility for enforcing account policy. The local SAM database does not “own” the account, so cached account passwords do not expire, and domain accounts can not be locked out when the domain is unavailable.

When establishing corporate policy for cached accounts, consider the remote user. They commonly log on with cached credentials from a laptop. To access corporate resources, the user establishes a Virtual Private Network (VPN) connection to the corporate network. Since logon occurs before the domain is available—the VPN has not yet been established—the user will never be prompted to change the password on the cached account.

This setting only affects workstations joined to a domain, and only impacts interactive logons with domain accounts. The workstation will not cache non-interactive log on information. Change this setting to zero to disable the caching of domain accounts in the local SAM database.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Interactive logon: Number of previous logons to cache (in case domain controller is not available)” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Interactive logon: Number of previous logons to cache (in case domain controller is not available)” setting in the “Database Setting” column to “0”.

3.2.1.31 Interactive logon: Prompt user to change password before expiration

Description: Should a user’s password be near its expiration date, the logon process warns the user and asks if they would like to change the password. Once the password has expired, the user will be required to change the password to complete the logon. This setting governs the window of convenience between the time when the system offers the user to change the password, and the time when they are required to change the password.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Interactive logon: Prompt user to change password before expiration)” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Interactive logon: Prompt user to change password before expiration)” setting in the “Database Setting” column to “5 days”.

3.2.1.32 Interactive logon: Require Domain Controller authentication to unlock workstation

Description: This setting results from a feature in Windows domain authentication; a further understanding of the behavior will help you determine the setting applicable to your organization. This setting does not affect standalone workstations.

The typical sequence for failure to unlock a workstation flows something like this:

1. The user repeatedly types in the wrong password.

2. For each password attempted, the workstation first compares the password to the cached password hash used for the original logon. If they do not match, it contacts the domain controller and attempts to log on.

3. After a predefined number of attempts, the domain controller locks out the account, and the workstation reports the account lockout.

At this point, most users will contact the system administrator and have the account lockout and perhaps the password reset. However, consider the persistent user that continues attempting to logon:

4. The user continues attempting to logon. Each time a bad password is entered, the workstation still compares it to the local cache; when the comparison fails, it contacts the domain controller, which also denies the logon.

5. Finally, the user enters the correct password. The workstation comparison to the local cache succeeds.

If this setting is disabled, the user then successfully unlocks the workstation. Even with a locked account, the user can then continue to access network resources for connections which were established and authenticated before the machine was locked—mail servers and file servers in particular.

Enabling this setting, however, adds an additional step after every successful workstation comparison with the local cache:

6. The workstation presents the credentials to the domain controller. Only if the domain controller authentication succeeds will the workstation be unlocked.

Enable this setting to protect against brute force password attacks through the screen saver. However, enabling it will hinder the user who locks and hibernates their workstation, and then attempts to resume when the domain controller is unavailable. Disabling this setting (or leaving it undefined) minimizes domain controller traffic.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Interactive logon: Require Domain Controller authentication to unlock workstation” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Interactive logon: Require Domain Controller authentication to unlock workstation” setting in the “Database Setting” column to “Enabled”.

Additional References:

For more information, see Microsoft Knowledge Base Articles 188700, “Screensaver Password Works Even If Account Is Locked Out” and 281250, “Information About Unlocking a Workstation”

3.2.1.33 Interactive logon: Require smart card

Description: Given a domain controller’s position in the network, additional two factor authentication methods may be considered in Specialized Security – Limited Functionality environments. Typically this includes smart card authentication, but can include other technologies. Smart cards are small credit card sized wafers containing memory chips that are running an embedded operating system and are used to provide additional authentication. Microsoft Windows Certificate services needs to be installed to provide for a Certification Authority for managing the Public Key Infrastructure [PKI].

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Interactive logon: Require smart card” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Interactive logon: Require smart card” setting in the “Database Setting” column to “Enabled” if you use smart cards. This is only recommended in a SSLF environment.

Additional References: For more information, a Berkeley case study on Smart Card implementation can be found at http://smartcard.berkeley.edu/documentation/SCPMaster20030319b.pdf.

3.2.1.34 Interactive logon: Smart card removal behavior

Description: When users authenticate with smart cards, the system can be set to lock or log out the user when the smart card is removed. Any setting other than “No Action” is acceptable.

In an environment that does not use Smart Cards, this setting has no effect.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Interactive logon: Smart card removal behavior” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Interactive logon: Smart card removal behavior” setting in the “Database Setting” column to “Force Logoff”.

3.2.1.35 Microsoft network client: Digitally sign communications (always)

Description: This setting applies specifically to communications using the Server Message Block (SMB) protocol. When enabled, the client will negotiate signed communications with any SMB server. If the server can not support SMB signing (typically servers prior to Windows 2000), communications will fail.

When possible, digitally sign client communication to protect against man-in-the-middle attacks, as it supports mutual authentication and protection against packet tampering.

SMB signing does not impact network bandwidth; however, CPU resources will be used in generating and verifying SMB signatures.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Microsoft network client: Digitally sign communications (always)” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Microsoft network client: Digitally sign communications (always)” setting in the “Database Setting” column to “Enabled”.

3.2.1.36 Microsoft network client: Digitally sign communications (if server agrees)

Description: This setting applies specifically to communications using the Server Message Block (SMB) protocol. When enabled, the client will negotiate signed communications with any server supporting SMB signing (typically Windows 2000 and later). Unsigned communications will still succeed with servers that do not support message signing.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Microsoft network client: Digitally sign communications (if server agrees)” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Microsoft network client: Digitally sign communications (if server agrees)” setting in the “Database Setting” column to “Enabled”.

3.2.1.37 Microsoft network client: Send unencrypted password to third-party SMB servers

Description: Would you like your Windows computer to send your password in clear text to another computer that requests authentication? The setting is disabled by default, and should remain so.

If you find an application that requires this setting to be enabled, please first send feedback to win2k-feedback@cisecurity.org so we can document it and contact the manufacturer. We will request a product redesign with better security, which will not require this behavior.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Microsoft network client: Send unencrypted password to third-party SMB servers” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Microsoft network client: Send unencrypted password to third-party SMB servers” setting in the “Database Setting” column to “Disabled”.

3.2.1.38 Microsoft network server: Amount of idle time required before disconnecting session

Description: This setting applies specifically to communications using the SMB protocol. When a client establishes a connection with an SMB server, they exchange credentials, perform authentication, and set aside resources to manage the connection. After a period of inactivity, the client or server may close the connection to conserve resources. When the client again attempts to use the SMB server, it reestablishes the connection without interaction with the user. The reconnection typically happens fast enough to hide the activity from the user.

Computers that do not share resources with other Windows computers are not affected by this setting.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Microsoft network server: Amount of idle time required before disconnecting session” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Microsoft network server: Amount of idle time required before disconnecting session” setting in the “Database Setting” column to “5 minutes”.

3.2.1.39 Microsoft network server: Digitally sign communications (always)

Description: Similar to 3.2.1.35, the workstation may require all SMB traffic to be digitally signed. Workstations act as servers when remote devices connect to published shares; many workstation management systems also use SMB protocols.

This setting will likely have less impact to the workstation than 3.2.1.35, since remote connections to workstations are typically well understood.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Microsoft network server: Digitally sign communications (always)” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Microsoft network server: Digitally sign communications (always)” setting in the “Database Setting” column to “Enabled”.

3.2.1.40 Microsoft network server: Digitally sign communications (if client agrees)

Description: Similar to 3.2.1.36, the workstation should request signed communications wherever possible. This option is enabled by default, and should remain enabled.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Microsoft network server: Digitally sign communications (if client agrees)” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Microsoft network server: Digitally sign communications (if client agrees)” setting in the “Database Setting” column to “Enabled”.

3.2.1.41 Microsoft network server: Disconnect clients when logon hours expire

Description: This setting only applies to workstations joined to a domain, as logon hours can not be set for local accounts. Additionally, this applies only to network connections established with the SMB protocol.

Domain accounts may be limited to specific hours when they may be used. By default, the domain controller only enforces these settings upon logon, but not after the session is established. With this setting enabled, should a user remotely log in to this workstation (the workstation acts as a server), the user’s network connections will be closed when their allotted time has been reached.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Microsoft network server: Disconnect clients when logon hours expire” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Microsoft network server: Disconnect clients when logon hours expire” setting in the “Database Setting” column to “Enabled”.

3.2.1.42 Network access: Do not allow storage of credentials or .NET Passports for network authentication

Description: This setting controls behavior of the “Stored User Names and Passwords” feature of Windows. This feature stores NTLM, Kerberos, Passport and SSL authentication; it should not be confused with the Internet Explorer authentication cache, since it is managed separately. Some documents refer to this setting as “Network Access: Do not allow Stored User Names and Passwords to safe passwords or credentials for domain authentication”.

Beware of the syntax for this option: Enabled keeps credentials out of the cache; Disabled allows storing user names and passwords.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Network access: Do not allow storage of credentials or .NET Passports for network authentication” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Network access: Do not allow storage of credentials or .NET Passports for network authentication” setting in the “Database Setting” column to “Enabled”.

3.2.1.43 Network access: Let Everyone permissions apply to anonymous users

Description: Many resources across the network are accessible to the “Everyone” group. This special group contains all accounts; however, it does not contain the anonymous user (null session, see section 3.1.1). Enabling this option adds the “null user” to the “Everyone” group, escalating privileges of this account. The “Everyone” group is assigned to many network resources by default.

This option is disabled by default and should remain disabled.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Network access: Let Everyone permissions apply to anonymous users” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Network access: Let Everyone permissions apply to anonymous users” setting in the “Database Setting” column to “Disabled”.

3.2.1.44 Network access: Named Pipes that can be accessed anonymously

Description: Named Pipes are communications channels between two processes. The process may or may not be located on the same computer, and communications are peer-to-peer rather than client-to-server. Each pipe is assigned an access control list.

This setting defines which pipes can be accessed remotely without authentication, and should be left blank. In order for this setting to take effect, you must enable 3.2.1.47, "Network Access: Restrict anonymous access to Named Pipes and Shares".

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "Network access: Named Pipes that can be accessed anonymously" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "Network access: Named Pipes that can be accessed anonymously" setting in the "Database Setting" column to "Disabled".

3.2.1.45 Network access: Remotely accessible registry paths

Description: This setting defines the registry paths which can be accessed from another computer.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "Network access: Remotely accessible registry paths" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "Network access: Remotely accessible registry paths" setting in the "Database Setting" column to an empty string "".

3.2.1.46 Network access: Remotely accessible registry paths and subpaths

Description: This setting defines the registry paths and corresponding child paths that can be accessed from another computer. Remote registry access depends on the remote registry service and requires authentication.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "Network access: Remotely accessible registry paths and subpaths" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Network access: Remotely accessible registry paths and subpaths” setting in the “Database Setting” column to an empty string “”.

3.2.1.47 Network access: Restrict anonymous access to Named Pipes and Shares

Description: When enabled, the anonymous restrictions on shares and named pipes take effect to prevent null sessions from accessing these resources.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Network access: Restrict anonymous access to Named Pipes and Shares” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Network access: Restrict anonymous access to Named Pipes and Shares” setting in the “Database Setting” column to “Enabled”.

3.2.1.48 Network access: Shares that can be accessed anonymously

Description: Access Control Lists restrict access to published network shares hosted by a server. Shares can be published to the “Everyone” group, but this does not include the unauthenticated null user. Adding specific shares to this list grants access to the unauthenticated user. Note that NTFS permissions on the share still apply. In order for this setting to take effect, you must enable 3.2.1.47, “Network Access: Restrict anonymous access to Named Pipes and Shares”.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Network access: Shares that can be accessed anonymously” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Network access: Shares that can be accessed anonymously” setting in the “Database Setting” column to “Enabled”.

3.2.1.49 Network access: Sharing and security model for local accounts

Description: Remote users often must present logon credentials to the workstation to gain access. Occasionally, they may present credentials for a local account on the workstation. In the “Classic” security model, even though a remote user is using local credentials, they still gain access based on restrictions for the local account. However, the

"Guest Only" model remaps the remote user to the guest account, so they will only be able to access resources available to guests.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "Network access: Sharing and security model for local accounts" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "Network access: Sharing and security model for local accounts" setting in the "Database Setting" column to "Guest Only".

3.2.1.50 Network security: Do not store LAN Manager hash value on next password change

Description: The SAM database typically stores a LANManager (LM) hash of account passwords. The SAM database should be secure on the workstation; however, if it is captured, the LM hash can be retrieved. Many vulnerabilities exist with the LM authentication model, and brute force attacks usually succeed with ease. Removing the LM hash from the SAM database helps protect the local account passwords. However, most Windows 9x clients only support LM authentication.

Beware of the syntax for this option: Enable this setting to keep the password secure; Disable this setting to weaken the password database and allow Windows 9x clients to log in remotely to the workstation.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "Network security: Do not store LAN Manager hash value on next password change" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "Network security: Do not store LAN Manager hash value on next password change" setting in the "Database Setting" column to "Enabled".

3.2.1.51 Network security: Force logoff when logon hours expire

Description: This setting is similar to 3.2.1.41, but reflects the client-side settings. This setting only applies to workstations joined to a domain, as logon hours can not be set for local accounts. The setting deals exclusively with connections using the SMB protocol, and not with the interactive logon session.

Enabling this feature will disconnect all client connections when logon time limits are reached. By default, the workstation only enforces logon hours during session setup, and not afterwards.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Network security: Force logoff when logon hours expire” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Network security: Force logoff when logon hours expire” setting in the “Database Setting” to “Enabled”.

3.2.1.52 Network security: LAN Manager authentication level

Description: Windows network authentication has changed considerably as various security vulnerabilities have been identified and fixed. The original LAN Manager (or LM) password hash is considered very weak, but is still used by most Windows 9x clients. Using commercially available software, and off-the-shelf computers, most LM password hashes can be used to reveal the actual password in a matter of days, or hours.

With the release of Windows NT 4.0, Microsoft developed NTLM authentication. Serious vulnerabilities made NTLM almost as easy to crack as LM, so NTLM version 2 (NTLMv2) was introduced. NTLMv2 provides significant improvements to security; when combined with strong password policy, accounts are well protected against brute force attacks. All of these authentication methods are incorporated into Windows 2000.

All authentication models work with a hash of the password, not the password itself. This presents challenges with down-level compatibility between operating systems. In order to smooth the transition, when one computer attempts to authenticate with another, the default behavior is to send the basic LM hash along with the more secure NTLM hash. This setting improves control over the response to an authentication challenge:

- Send LM & NTLM responses
- Send LM & NTLM, Use NTLMv2 session security if negotiated
- Send NTLM response only
- Send NTLMv2 response only
- Send NTLMv2 response only\refuse LM
- Send NTLMv2 response only\refuse LM & NTLM

The default option, and the weakest option, is the first: send LM & NTLM responses. As a result, using NTLM is ineffective because both protocols are sent together. In order to take a much more effective stand to protect network authentication, set LAN Manager Authentication Level to “Send NTLMv2 response only”.

Enabling this setting may have adverse effects on your ability to communicate with other Windows machines unless the change is made network-wide. If you find that you are unable to require a certain level of LM Authentication, back down to “Send LM & NTLM – Use NTLMv2 session security if negotiated” and try your network authentication again.

Communication with Windows 9x/Me machines requires the DSCLIENT.EXE utility from the Windows 2000 installation CD.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Network security: LAN Manager authentication level” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Network security: LAN Manager authentication level” setting in the “Database Setting” column to “Send NTLMv2 response”.

3.2.1.53 Network security: LDAP client signing requirements

Description: Similar to the SMB protocol, the LDAP protocol supports signing. LDAP, “Lightweight Directory Access Protocol,” provides one means for the client to talk to active directory. LDAP protocol is text-based, but supports authentication to gain access to sensitive sections of the directory. Require signing to provide the assurance of mutual authentication for this communications channel.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Network security LDAP client signing requirements” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Network security LDAP client signing requirements” setting in the “Database Setting” column to “Require Signing”.

3.2.1.54 Network security: Minimum session security for NTLM SSP based (including secure RPC) clients

Description: NTLM authentication can provide a security service to manage connection between various clients and servers, including through the Remote Procedure Call (RPC) service. Windows 2000 improved the security model for secure, authenticated client-server communications; this setting manages the new features for communications established by this workstation.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Network security Minimum session security for NTLM SSP based (including secure RPC) clients” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Network security Minimum session security for NTLM SSP based (including secure RPC) clients” setting in the “Database Setting” column to require: “Message integrity”, “Message confidentiality”, “ntlmv2 session security” and “128-bit encryption”.

3.2.1.55 Network security: Minimum session security for NTLM SSP based (including secure RPC) servers

Description: Similar to 3.2.1.54, this setting manages features for communication services provided by this workstation to other computers.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Network security Minimum session security for NTLM SSP based (including secure RPC) servers” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Network security Minimum session security for NTLM SSP based (including secure RPC) servers” setting in the “Database Setting” column to require: “Message integrity”, “Message confidentiality”, “ntlmv2 session security” and “128-bit encryption”.

3.2.1.56 Recovery console: Allow automatic administrative logon

Description: The Recovery Console, new to Windows 2000, XP and 2003, provides a limited command-line access to an otherwise unbootable operating system.

The console allows access to the NTFS file system, which does not natively allow access when the operating system becomes unbootable. Other third-party applications have been developed to perform this action as well, but the Recovery Console is part of the operating system. It can be installed from the Windows 2000 CD with the “d:\i386\winnt32.exe /cmdcons” command. It can also be run directly from the Windows 2000 installation CD. By default, the recovery console will allow full access to the system after the user logs in with the password of the Administrator account.

The Recovery Console does not grant full and unrestricted access to the operating system by default. It does require that you log on using the password of the default Administrator account. Keep in mind that this must be the local administrator account, not just a member of the local administrators group. Also, the policy for renaming the administrator account does not apply to the recovery console, and that password must be used.

If configured, booting to the recovery console could result in automatic logon, and bypass the need for the password of the administrator account. Since this gives administrator access to anyone who can reboot the computer, the setting is generally disabled.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Recovery Console: Allow automatic administrative logon” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Recovery Console: Allow automatic administrative logon” setting in the “Database Setting” column to “Disabled”.

3.2.1.57 Recovery console: Allow floppy copy and access to all drives and all folders

Description: By default, the Recovery Console only allows access to the root folder of each drive, and the operating system folder (typically C:\Windows). The console also prevents copying files from the hard drive onto removable media. Although this protection can be bypassed by enabling floppy copy and drive access, the setting is enabled by default and should remain disabled.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Recovery Console: Allow floppy copy and access to all drives and all folders” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Recovery Console: Allow floppy copy and access to all drives and all folders” setting in the “Database Setting” column to “Disabled”.

3.2.1.58 Shutdown: Allow system to be shut down without having to log on

Description: Some systems run critical processes and should only be shut down by authorized users. Occasionally, special processes could be evoked during system startup, sometimes even trojaned processes. In environments where abnormal system reboots could cause problems, require a logon prior to reboot.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Recovery Console: Allow system to be shut down without having to log on” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security

Options”. Now set the "Recovery Console: Allow system to be shut down without having to log on” setting in the “Database Setting” column to “Disabled”.

3.2.1.59 Shutdown: Clear virtual memory pagefile

Description: Virtual memory extends the physical memory available to the CPU. As data and applications fill the available physical memory, the operating system writes less-frequently used pages of memory out to disk, into the virtual memory pagefile. This greatly extends the amount of “virtual” memory available to the computer.

Since the pagefile contains information that was in memory, it potentially holds a great deal of information useful for an attacker. Digging through the pagefile can reveal SSL web pages, queries set from the client to databases, sometimes even user ids and passwords from poorly written applications.

The workstation does not clean this information from the pagefile on shutdown. Although the file can not be accessed when booted in Windows, anyone booting the workstation to an alternate operating system (e.g., from a boot CD) may access the page file.

Enabling this options provides greater security by erasing the data during normal operations; however, this may also significantly increase the time required to shut down the computer. When enabled, the hibernation file (hiberfil.sys) is also cleaned on shutdown.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "Shutdown: Clear virtual memory pagefile” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "Shutdown: Clear virtual memory pagefile” setting in the “Database Setting” column to “Enabled”.

3.2.1.60 System cryptography: Force strong key protection for user keys stored on the computer

Description: Strong Key protection helps keep private keys safe when they are stored on the local computer by locking the key with a password. This option requires users to enter the password when the key is first used, or every time the key is used. The password is not synchronized with the domain account password. This option applies to user keys which are managed through the data protection Application Programming Interface (API).

Often users use a third-party tool such as Pretty Good Privacy (PGP) or Gnu Privacy Guard (GPG) to store private user keys. When this setting is enabled, the Microsoft private key store simulates the behavior of these tools by requiring a password to unlock the key. However, the Microsoft protection lacks robust features of these tools such as specifying the strength of the password and timing out the cached password.

Enabling strong key protection helps containerize and protect data to guard against stolen or hijacked computers. If you step away from your machine but leave it unlocked, another person can sit down at the machine and act as you, but they will not be able to read your secure e-mail or access an internet site that uses your client-side certificate.

By assigning a unique password to client certificates, you increase the burden on the user to remember passwords. As the number of passwords increases, it becomes more likely that the user will write down passwords, and may increase your exposure to password attacks.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "System cryptography: Force strong key protection for user keys stored on the computer” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "System cryptography: Force strong key protection for user keys stored on the computer” setting in the “Database Setting” column to “User must enter a password each time they use the key”.

References: For more information about the data protection API, see Microsoft’s knowledge base article 309408, “Troubleshooting the Data Protection API (DPAPI),” http://support.microsoft.com/default.aspx?scid=kb;en-us;309408.

3.2.1.61 System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing

Description: FIPS stands for “Federal Information Processing Standards”. The National Institute of Standards and Technology (NIST) maintains the standards, available online at http://www.itl.nist.gov/fipspubs/index.htm. Although the operating system can support a variety of hashing and encryption algorithms, only the following are FIPS compliant:

- Secure Hash Algorithm (SHA-1) for hashing
- Triple Data Encryption Standard (DES) for encryption
- RSA for key exchange and authentication.

Only these algorithms are used when the workstation requires FIPS compliant algorithms. With this setting enabled, the encrypting file system (EFS) will use triple DES rather than the default DESX.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing” setting in the “Database Setting” column to “Enabled”.

3.2.1.62 System objects: Default owner for objects created by members of the Administrators group

Description: When a member of the Administrators group creates an object (file, directory, account, or any object which obtains and ACL from the operating system), an owner will be assigned. Normally, the account which created the object is assigned as the owner; however, changing this option allows assignment to the “Administrators Group” rather than an individual account.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "System objects: Default owner for objects created by members of the Administrators group” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now et the "System objects: Default owner for objects created by members of the Administrators group” setting in the “Database Setting” column to “Administrators group”.

3.2.1.63 System objects: Require case insensitivity for non-Windows subsystems

Description: The Windows operating systems ignore case when accessing resources; for example, “C:\Windows”, “C:\WINDOWS” and “c:\windows” all refer to the same directory. However, the Windows kernel allows interfaces with other case-sensitive operating systems (e.g., Unix). Enabling this setting causes the interoperability features to be case-insensitive as well.

This setting has no effect when the computer communicates only with other Windows systems.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "System objects: Require case insensitivity for non-Windows subsystems” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "System objects: Require case insensitivity for non-Windows subsystems” setting in the “Database Setting” column to “Enabled”.

3.2.1.64 System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)

Description: This setting actually digs deep into the operating system behavior and should be left at the default setting (Enabled) unless explicitly required.

“Internal system objects” are shared physical and logical resources such as semaphores and DOS device name; the objects all are created with access control lists (ACLs). When enabled, the ACL allows other non-administrative system processes to query internal system objects, but will not allow them to modify them.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)” setting in the “Database Setting” column to “Disabled”.

3.2.1.65 System settings: Optional subsystems

Description: Here you can define subsystems which support running applications. The default entry of “POSIX” allows the POSIX subsystem to run. Defining this option but leaving the list blank will effectively disable the POSIX subsystem, which is only useful for Unix emulation services running on Windows.

Subsystems can spawn processes which access multiple user sessions. The poorly written subsystem may allow a process to escalate privileges by accessing another account’s process.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "System settings: Optional subsystems” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "System settings: Optional subsystems” setting in the “Database Setting” column to “POSIX”.

3.2.1.66 System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies

Description: Software restriction policies define the software that is allowed to run on a computer. These policies help protect against malicious code introduced into the environment. Policies can be set based on a hash of the executable, the path to the executable, the source internet zone (for MSI packages only), or based on the certificate used to sign the executable.

This setting enables certificate based software restriction policies. Every executable is checked for an authenticode signature, and the signature is verified against a list of “trusted publishers” and a certificate revocation list (CRL). If software restriction policies are in use, this rule can determine how executables (*.exe files only) are grouped into access rights blocks.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies” setting in the “Database Setting” column to “Disabled”.

References: http://technet2.microsoft.com/windowsserver/en/library/ac308f08-bf6a-4013-84ac-6fafcdb63e0a1033.mspx?mfr=true

3.2.1.67 MSS: (AFD DynamicBacklogGrowthDelta) Number of connections to create when additional connections are necessary for Winsock applications (10 recommended)

Description: Windows socket applications which support a large number of connections use AFD.sys to manage connection backlog. Four settings control how this backlog is handled.

Should all the existing connections be used, this setting determines how many additional connections are created. If this is set too large, the computer could be susceptible to a SYN-flood or similar resource exhaustion attack.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "MSS: Number of connections to create when additional connections are necessary for Winsock applications” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "MSS: Number of connections to create when additional connections are necessary for Winsock applications” setting in the “Database Setting” column to “10”.

3.2.1.68 MSS: (AFD EnableDynamicBacklog) Enable dynamic backlog for Winsock applications

Description: This setting is the overall control for AFD dynamic backlog. When this is set to disable, dynamic backlogging is turned off.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "MSS: (AFD EnableDynamicBacklog) Enable dynamic backlog for Winsock applications" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "MSS: (AFD EnableDynamicBacklog) Enable dynamic backlog for Winsock applications" setting in the "Database Setting" column to "Enabled".

3.2.1.69 MSS: (AFD MaximumDynamicBacklog) Maximum number of 'quasi-free' connections for Winsock applications

Description: A "quasi-free" connection is one in which the SYN packet is sent, but the full TCP 3-way connection handshake is not yet complete. This setting defines the number of uninitiated and the number of quasi-free connections per listening endpoint.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "MSS: (AFD MaximumDynamicBacklog) Maximum number of 'quasi-free' connections for Winsock applications" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "MSS: (AFD MaximumDynamicBacklog) Maximum number of 'quasi-free' connections for Winsock applications" setting in the "Database Setting" column to "10".

3.2.1.70 MSS: (AFD MinimumDynamicBacklog) Minimum number of free connections for Winsock applications (20 recommended for systems under attack, 10 otherwise)

Description: This setting defines the minimum number of free connections that can exist before a new thread is created to open up additional connections.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "MSS: (AFD MaximumDynamicBacklog) Minimum number of free connections for Winsock applications" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security

Options”. Now set the "MSS: (AFD MaximumDynamicBacklog) Minimum number of free connections for Winsock applications” setting in the “Database Setting” column to “10”.

3.2.1.71 MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)

Description: If a Windows computer has two valid networking devices installed, it can be configured to act as a router or a firewall, and pass network traffic from one interface to another. Whether this is the intended purpose or not, it can be done on any Windows computer. “Source Routing” traffic that passes through such a router can bypass certain routing rules by “spoofing” the device to think malicious network activity came from the protected side. Set this value to 2 in order to drop all source routed packets.

You can easily check your machines to see if they allow source routing. To find out if the machine at address 10.1.1.20 on the File & Print services VLAN can route packets to the machine at 10.1.2.21 on the Human Resources VLAN, from the command prompt type

```
Ping –j 10.1.1.20 10.1.2.21
```

Suppose that you issue this command from client address 10.1.3.22 on the Sales Force VLAN, and network restrictions placed on routers prevent the Sales Force VLAN (10.1.3.x) from accessing the Human Resources VLAN (10.1.2.x). If this ping succeeds, you bypass those access restrictions by routing packets to Human Resources via the File & Print services VLAN (10.1.1.x).

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)” setting in the “Database Setting” column to “Highest protection, source routing is completely disabled”.

3.2.1.72 MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)

Description: When one TCP/IP Default Gateway fails, it is possible to force one computer to use a second default gateway to complete the route path. In most cases, computers are not set up with multiple default gateways, relying on redundant routers instead.

If an attacker can manipulate your default gateway, and this setting is not set to zero, he could route your network traffic to an alternate address. Set this value to zero to protect against this kind of attack.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)” setting in the “Database Setting” column to “0”.

3.2.1.73 MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes

Description: In order to prevent network ICMP traffic from being redirected from one computer to another, set the EnableICMPRedirect value to zero. There is some confusion as to whether or not the value name is pluralized.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes” setting in the “Database Setting” column to “0”

References: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q293626.

3.2.1.74 MSS: (EnablePMTUDiscovery) Allow automatic detection of MTU size (possible DoS by an attacker using a small MTU)

Description: When data is transferred across a network, the data is broken down into packets. These packets are not always a uniform size. When these packets are broken down into smaller sizes, they are supposed to be reassembled at the other end of a network route in the same order. This does not always go as planned, and can used in some network attacks.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "MSS: (EnablePMTUDiscovery) Allow automatic detection of MTU size (possible DoS by an attacker using a small MTU)” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security

Options". Now set the "MSS: (EnablePMTUDiscovery) Allow automatic detection of MTU size (possible DoS by an attacker using a small MTU)" setting in the "Database Setting" column to "0".

References: More details are available at http://support.microsoft.com/?kbid=315669.

3.2.1.75 MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers

Description: By default, a computer running NetBIOS will release its name upon request. In order to protect against malicious name-release attacks, set this value to 1. Microsoft also references in at least one place that this is for Windows 2000 Service Pack 2 or greater.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers" setting in the "Database Setting" column to "1".

3.2.1.76 MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure DefaultGateway addresses (could lead to DoS)

Description: This setting prohibits the workstation from caching router advertisements. Since router advertisements propogate through UDP, they can easily be spoofed.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure DefaultGateway addresses (could lead to DoS)" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure DefaultGateway addresses (could lead to DoS)" setting in the "Database Setting" column to "Disabled".

3.2.1.77 MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)

Description: One of the first methods of launching Denial of Service attacks was to send a flood of incomplete 3-way handshake requests. Each time the incomplete request was received by the target, a small portion of the target's resources were set aside, waiting for the request to finish. When all of the resources were set aside, the target machine was no longer able to serve any more requests, and further service was denied.

In order to prevent the success of this attack, set the SynAttackProtect value to 2, which allows the operating system to limit the amount of resources that are set aside until the 3-way handshake is completed. Setting SynAttackProtect to 1 provides minimal security, but for maximum protection, set it to 2.

The next few settings also provide a measure of protection against Denial of Service or Distributed Denial of Service attacks.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)" setting in the "Database Setting" column to "2".

3.2.1.78 MSS: (TCPMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged

Description: In a typical TCP handshake, the client begins the transmission by sending a single SYN packet to the server; the server responds with a SYN-ACK packet, and the client completes the handshake with an ACK packet. In some cases, the client does not respond to the server's SYN-ACK packet. This setting defines how many times the server resends the SYN-ACK packet.

The server waits 3 seconds after the initial packet is sent, then doubles the wait time after each successive packet. With this set to 3, the server sends the packet, waits 3 seconds, resends, waits 6 seconds, resends and waits 12 seconds before finally abandoning the connection after 3 + 6 + 12 = 21 seconds. If this setting is set to zero, the server will wait three seconds for the client's ACK packet, and then abandon the connection without resending the SYN-ACK packet.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "MSS: (TCPMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "MSS: (TCPMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged" setting in the "Database Setting" column to "0".

3.2.1.79 MSS: (TCPMaxDataRetransmissions) How many times unacknowledged data is retransmitted

Description: This setting works similar to 3.2.1.783.2.1.78; however, this refers to retransmission of individual data packets within an existing TCP stream.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "MSS: (TCPMaxDataRetransmissions) How many times unacknowledged data is retransmitted" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "MSS: (TCPMaxDataRetransmissions) How many times unacknowledged data is retransmitted" setting in the "Database Setting" column to "3"

3.2.1.80 MSS: (TCPMaxPortsExhausted) How many dropped connect requests to initiate SYN attack protection

Description: This setting defines the point at which SYN flood protection begins by measuring the number of connections that were refused because resources were not available to handle the request.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now view the "MSS: (TCPMaxPortsExhausted) How many dropped connect requests to initiate SYN attack protection" setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on "Security Options". Now set the "MSS: (TCPMaxPortsExhausted) How many dropped connect requests to initiate SYN attack protection" setting in the "Database Setting" column to "5".

3.2.1.81 MSS: Disable Autorun for all drives

Description: Although it is convenient for applications to automatically run when Windows Explorer opens up, it can also cause applications to be executed against the wishes of an administrative user, and exploiting that privilege. Set this value to 255 to prevent any type of drive from automatically launching an application from Windows Explorer.

If malicious software is written to a CD, it can be executed by Windows Explorer just by putting the CD in the drive. Set this value to zero to prevent any applications from automatically launching from the CD-ROM drive.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "MSS: Disable Autorun for all drives” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "MSS: Disable Autorun for all drives” setting in the “Database Setting” column to “255”.

3.2.1.82 MSS: Enable Safe DLL search mode (recommended)

Description: This setting modifies the way in which Windows locates driver files (.dlls). A value of 0 forces the operating system to search the current directory first; when set to 1, the system searches the windows system directory first.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "MSS: Enable Safe DLL search mode (recommended)” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "MSS: Enable Safe DLL search mode (recommended)” setting in the “Database Setting” column to “0”.

3.2.1.83 MSS: Enable the computer to stop generating 8.3 style filenames

Description: In order for backwards compatibility with 16-bit systems, it is possible to generate 8-character compatible names for every file on the system. In this case, an attacker can reference any file on the system with only 8 characters. Disable this feature to force clients to reference files by their full name.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "MSS: Enable the computer to stop generating 8.3 style filenames” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "MSS: Enable the computer to stop generating 8.3 style filenames” setting in the “Database Setting” column to “Enabled”.

3.2.1.84 MSS: How often keep-alive packets are sent in milliseconds

Description: The KeepAliveTime determines how often the network subsystem attempts to verify that a TCP session is still active. The setting of 300,000 works out to one request every five minutes.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "MSS: How often keep-alive packets are sent in milliseconds” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "MSS: How often keep-alive packets are sent in milliseconds” setting in the “Database Setting” column to “300,000 or one request every 5 minutes”.

3.2.1.85 MSS: Percentage threshold for the security event log at which the system will generate a warning

Description: With Windows 2003, it is possible to create an event when the event log is near full. When the security event log reaches this percentage, a 523 event is cut which notifies the log is almost full.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "MSS: Percentage threshold for the security event log at which the system will generate a warning” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "MSS: Percentage threshold for the security event log at which the system will generate a warning” setting in the “Database Setting” column to “80%”.

3.2.1.86 MSS: The time in seconds before the screen saver grace period expires

Description: By default, Windows has a brief period between when the screen saver takes control of the screen until the time the system actually locks. The default timeout period is five seconds.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now view the "MSS: The time in seconds before the screen saver grace period expires” setting.

Remediation: Expand "Security Configuration and Analysis" in the Console Root of the Microsoft Management Console. Then expand "Local Policies" and click on “Security Options”. Now set the "MSS: The time in seconds before the screen saver grace period expires” setting in the “Database Setting” column to “0”.

4 Additional Security Protection

Many of the security related settings listed above fell neatly into categories that were well defined, easy to implement, and easy to find. Beyond that, there are other requirements that do not fit into every mold – these are the things that make every computer unique. These may present the greatest challenge to securing a computer because these are more open-ended in nature. For lack of a better description, the pages that follow describe the realm that would fall into the category “*other*”.

4.1 Available Services

Every piece of code that executes on a computer exists in a process. Many of these processes begin as “Services”. You can view a list of processes by right-clicking “My Computer”, and click “Manage”. Expand “Services and Applications” and click “Services”. Group policy allows you to specify that these services start either at boot time (Automatic), when required by another service or process (Manual) or that they do not start (Disabled).

Permissions on services listed here should be set to **Administrators: Full Control; System: Full Control; Interactive Users: Read.** Set permissions on services using the Security template that accompanies the CIS Windows Scoring Tool. Note that these permissions define which users can manage the services, not the actual permissions the services themselves run under. Defining “Administrators: Full Control” for the services means that only administrators can start and stop the service, but it does not mean that the service runs with administrative rights.

Many experts question how much security “value” you get by assigning permissions to services. The argument is usually something like “Well, if they’ve gotten that far onto your system, you have already lost.” While there is some truth to that, we are limited by the fact that Microsoft security templates have a limitation – in order to set the state of a service, you must also set the permissions.

Windows XP introduced two additional service accounts which are also available in Windows 2003. In addition to the “Local System” account, services can also run under the “Network Service” account and the “Local Service” account.

- The Local System account provides unlimited administrative access to the local machine, and should be considered a highly privileged account. This account is also able to access network resources; when doing so, it authenticates to the resource using the machine account.
- The Network Service account does not have administrative access on the local machine; rather, it operates as a standard user account. However, this account is designed for services that may need access to network resources, and can authenticate to them using the machine account.

- The Local Service account can only access resources on the local machine in the context of a standard user account. Although this account can still make connections across the network, it only does so with using the "null user" account (see 3.1.1).

Whenever possible, assign services to run with the minimum privileges possible—first try Local Service, then Network Service before allowing Local System access. Keep in mind that services running under these accounts may not have access to resources (files, registry keys, etc.) protected by an Access Control List (ACL). To change the account for a service, select "Start > Control Panel > Administrative Tools > Services". Right-click on the service name and select "Properties", then click the "Log On" tab. To use the local service accounts, click the "this account" radio button and type "NT AUTHORITY\LocalService." Leave the password blank and click OK to save changes.

Services can be set to Automatic, Manual or Disabled through group policy. However, exceptions to service settings can be difficult to manage through group policy, so care must be taken when designing control of services across the domain. When set to "manual", services will sometimes start when needed, but not always. Manual services are often started by management tools that use the service; however, Windows 2003 services should already be set to "manual" when the service will support it. Changing these settings could cause dependent applications to fail.

Accounts under which services run are not specified through Group Policy, and are not graded by the CIS Scoring Tool.

Due to the large number of services available with Windows 2003, only those services which have been disabled are mentioned below. For Microsoft references on Windows 2003 services, see "System Services for the Windows Server 2003 Family and Windows XP Operating Systems",http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/svrxpser_7.mspx

4.1.1 Alerter (Alerter)

Description: The alerter service is normally used to send messages between processes on one computer "alerting" the status of certain functions to the user's console, including the execution of print jobs. It also works in conjunction with the Messenger service to send these same messages between computers on a network.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the Alerter services status.

Remediation: Start > Run > cmd.exe and type "net stop alerter".

4.1.2 Client Service for NetWare (NWCWorkstation)

Description: The Netware Client Service allows interoperability between the system and NetWare file & print resources. Disable this service if NetWare resources are not used in your organization.

Recommendation Level: 1

Scoring Status: Not Scorable.

Audit: Start > Run > "Services.msc" and view the NWCWorkstation services status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.3 ClipBook (ClipSrv)

Description: The Clipbook service is used to share clipboard information between computers on a network. The service has been available through many versions of Windows but is rarely used. It shares data through the Network Dynamic Data Exchange (NetDDE) protocol.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the ClipSrv status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.4 Fax Service (Fax)

Description: The fax service is used for the unattended reception of incoming faxes. It is not required for the sending, or manual reception of faxes. It does require that a computer be left running all the time, and have the modem set to auto-answer.

Generally speaking, with the low cost of dedicated fax machines, the secure answer to most faxing needs would be to have a dedicated fax machine to receive faxes, while still using the computer to manually send faxes when appropriate.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the Fax status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.5 File Replication (NtFrs)

Description: The File Replication Service (FRS) maintains a consistent file share replicated across multiple servers. This is used to maintain the SYSVOL share on domain controllers. FRS can be used to create pools of relatively static documents on Local Area Networks, and replicate changes across slow links, rather than keeping all the documents stored in one location. Users then access the file stored on the local network, and only changes to the files are sent across the link.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the NtFrs status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.6 File Server for Macintosh (MacFile)

Description: This service enables Macintosh computers to access files on Windows 2003 file servers

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the MacFile status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

.

4.1.7 FTP Publishing Service (MSFtpsvc)

Description: The FTP Publishing Service is part of the Internet Information Server suite of Internet applications. It is not installed by default. It is used for making files on your local machine available to other users on your network or the Internet.

Generally speaking, workstations do not share files with other computers. This service should be disabled, or removed. If it is going to be installed, it should be properly maintained, which is a subject beyond the scope of this benchmark.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the msftpsvc status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.8 Help and Support (helpsvc)

Description: The Help and Support service allows the Help and Support center to run on the local computer. When disabled, the user will not be able to start the “Help and Support center”, although they will still be able to open up the help files on disk in the Windows\Help folder.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the helpsvc status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.9 HTTP SSL (HTTPFilter)

Description: This service enables Secure Socket Layer (SSL) transport of the HTTP protocol through Internet Information Services (IIS)

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the HTTPFilter status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.10 IIS Admin Service (IISADMIN)

Description: Also part of the IIS suite of services, the IIS Admin Service manages the other IIS services. If this service is not running, the other services that are part of the IIS suite will not function either. Disable this service. If possible, this should be removed from workstations.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the IISADMIN status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.11 Indexing Service (cisvc)

Description: This service indexes files on the system in an attempt to improve search performance using a flexible query language. However, the service may occasionally consume excessive resources when compared to its usefulness.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the cisvc status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.12 License Logging Service (LicenseService)

Description: The license monitoring service watches licensing of some Microsoft software running on the computer.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the LicenseService status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.13 Messenger (Messenger)

Description: The Messenger service works in tandem with the Alerter service. It allows Alerter services of multiple computers to send alerts to each other over a network. Most users can live without the messenger and alerter services and still accomplish the tasks they need to do in the course of a normal day.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the Messenger status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.14 Microsoft POP3 Service

Description: The POP3 Service enables a Post Office Protocol version 3 service on the computer. This plain text unencrypted protocol allows a user to retrieve messages from a mail box. It is typically used hand-in-hand with the Simple Mail Transport Protocol (SMTP), necessary for sending messages.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the "POP3 service" status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.15 NetMeeting Remote Desktop Sharing (mnmsrvc)

Description: Microsoft has made one of the better collaboration tools that is available on the market today, but at the same time they took that tool – NetMeeting – and tried to make it into a remote control utility for help desk personnel to take control of your computer in time of need. In a world of hacker attacks and buffer overflows, it seems like only a matter of time before an exploit is discovered, or it is just abused. If you don't have a dedicated help desk, or your help desk doesn't use NetMeeting Remote Desktop Sharing, disable this service. If your organization requires this service, it should understand that there may be a risk involved.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the mnmsrvc status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.16 Network Connections

Description: This service manages all the objects in the “Network Connections” folder in Explorer. If set to manual, the service will automatically start when required.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the netman status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.17 Network News Transport Protocol (NNTP) (NntpSvc)

Description: The NNTP service allows an IIS server to host news group discussions. The discussions can be hosted locally, or can be forwarded to clients from external news servers. Most popular mail clients include a news reader.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the NntpSvc status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.18 Print Server for Macintosh (MacPrint)

Description: The MacPrint service allows a Macintosh client to print to printers connected to this machine.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the MacPrint status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.19 Print Spooler (Spooler)

Description: The Spooler service is used to queue documents before sending them to a printer managed by this device. Only print servers or servers with attached printers need to run this service.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the Spooler status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.20 Remote Access Auto Connection Manager (RasAuto)

Description: When attempting to access a resource on a remote network, the Auto Connection Manager service will automatically start the network connection when necessary. This should not be necessary for a server, since servers should have network connections permanently configured for persistent connections.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the RasAuto status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.21 Remote Access Connection Manager (RasMan)

Description: The RasMan service is necessary for creating remote network connections. These do not include an attached Ethernet interface. This service is required for Internet Connection Sharing.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the RasMan status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.22 Remote Administration Service

Description: The Remote Administration Service will perform various administrative tasks requested by the Remote Server Manager. The Remote Server Manager service will start this when needed.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the RasMan status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual. Only disable for a Specialized Security – Limited Functionality (SSLF) environment.

4.1.23 Remote Desktop Help Session Manager (RDSessMgr)

Description: This service supports the Remote Assistance functionality. Disable the service to prohibit the use of Remote Assistance.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the RDSessMgr status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.24 Remote Installation (BINLSVC)

Description: Also known as the “Boot Information Negotiation Layer” service, the Remote Installation service should run only on servers used to manage client boot requests. These requests are part of the Pre-boot eXecution Environment (PXE); a Remote Installation server forms part of the infrastructure necessary to boot workstations from the network and push down an operating system image.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the BINLSVC status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.25 Remote Procedure Call (RPC) Locator (RpcLocator)

Description: This service can be used by remote clients that use the RpcNs API to locate services on a remote computer. The service is not used for local identification of services. The service opens up a listener on TCP port 135.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the RpcLocator status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.26 Remote Registry Service (RemoteRegistry)

Description: The Windows Registry is essentially a database of settings and configuration options that affect almost every function of a Windows computer. It determines how everything behaves at startup, shutdown, and everything in between. The purpose of the Remote Registry Services is to expose that database to the rest of the network through a NetBIOS connection.

As frightening as that sounds, this service is enabled by default on every Windows computer deployed since the advent of Windows 95. A majority of remote administration tools have been written to take advantage of the Remote Registry Service to perform functions that would normally require a portion of their application to be installed locally.

Because of its widespread distribution, and its initial purpose, and the fact that it is still only protected by a username and password, the Remote Registry Service is responsible for opening the doors to uninvited guests as well as the remote management utilities it is used to support. Disable this service to prevent remote access to the system registry.

WARNING: By disabling this service, you are cutting any ability for support personnel or domain administrators to remotely manage your computer unless there is another application already installed on your computer to allow those functions. Be wary that this can break a large number of enterprise-wide applications. Another way of managing the remote registry instead of shutting down the service is to restrict who can access it via registry settings. You can restrict anonymous access to the registry by modifying the HKEY_LOCAL_MACHINE/System/CurrentControlSet/Control/SecurePipeServers/Winreg key. The best solution is still to disable this service altogether if it is not needed though.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the RemoteRegistry status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.27 Remote Server Manager (AppMgr)

Description: The AppMgr service uses the Windows Management Interface (WMI) to manage remote administration alerts and tasks.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the AppMgr status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.28 Remote Server Monitor (Appmon)

Description: The Appmon service can monitor critical resource information on remotely managed servers.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the Appmon status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.29 Remote Storage Notification (Remote_Storage_User_Link)

Description: The Remote Storage User Link is used to notify a user when the file being accessed is only available from alternate storage media.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the Remote_Storage_User_Link status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.30 Remote Storage Server (Remote_Storage_Server)

Description: The Remote Storage Server service allows hierarchical storage based on storage cost and frequency of use. For more information on hierarchical storage, see Microsoft's documentation on "Managing Data with Removable and Remote Storage."

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the Remote_Storage_Server status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.31 Simple Mail Transport Protocol (SMTP) (SMTPSVC)

Description: Workstations are not normally used as SMTP mail servers. This service is installed as part of the IIS suite of applications. It should be disabled or removed entirely.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the SMTPSVC status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.32 SNMP Service (SNMP)

Description: The Simple Network Management Protocol (SNMP) has long been the accepted standard for remote management through all network devices – routers, hubs, Unix, and Windows alike. It was recently discovered that SNMP has been proliferating a dangerously exploitable flaw for the past ten years or so. If you do not have a system actively using SNMP for remote management, disable it or remove it from the system.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the SNMP status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.33 SNMP Trap Service (SNMPTRAP)

Description: Another part of the SNMP protocol is the SNMP Trap service. Just like its counterpart, it should be disabled and/or removed.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the SNMPTRAP status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.34 Telephony (TapiSrv)

Description: The telephony service handles all the dial-up activity on the computer.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the TapiSrv status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.35 Telnet (TlntSvr)

Description: The Telnet service is not often installed on workstations. It is used for remote management of network devices, and offers a command-shell based form of network access to a computer. This is all well and good, but the traffic transferred by Telnet is not protected or encrypted in any way. If this is a requirement, take the time to look into a Secure Shell (SSH) remote management solution to fulfill your needs in a more secure manner. It is well worth the time and expense.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the TlntSvr status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.36 Terminal Services (TermService)

Description: Terminal services allow a remote graphical interface to the workstation. Similar to pcAnywhere or Virtual Network Client (VNC) software packages, Terminal Services share using the Remote Desktop Protocol (RDP). Normal use of the terminal service on a workstation terminates the existing interactive logon session; however, if remote assistance is enabled, any existing session can be shared between two computers.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the TermService status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.37 Trivial FTP Daemon (tftpd)

Description: Trivial FTP (tftp) offers a lightweight, unauthenticated version of the FTP protocol. The service is typically used for bootstrapping devices during automated startup, and is part of the requirements for a Remote Installation service (see 4.1.24). However, tftp is also a favorite protocol for propagation of worms and Trojan horse applications, and should be disabled wherever possible.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the tftpd status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.38 Volume Shadow Copy (VSS)

Description: The Volume Shadow Service implements Volume Shadow Copies of files stored on network shares to be used for revisioning and backup purposes. It can be thought of as the “network recycle bin”. Note that this will break some backup systems and is not recommended without investigation.

Recommendation Level: 2

Scoring Status: Scorable.

Audit: Start > Run > “Services.msc” and view the VSS status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

References: http://www.windowsnetworking.com/articles_tutorials/Windows-Server-2003-Volume-Shadow-Copy-Service.html

4.1.39 Wireless Configuration (WZCSVC)

Description: The Wireless Zero Configuration service is used to effortlessly configure wireless networking service. If the target device does not have a wireless network card, this service should be disabled.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the WZCSVC status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.40 Windows Media Services (wmserver)

Description: The Windows Media Services service provides streaming media over IP-based networks. If the target device does need this service it , this service should be disabled as it has a history of security problems.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the WMSERVER status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.41 World Wide Web Publishing Service (W3SVC)

Description: The grand-daddy of all exploitable services is Microsoft's World Wide Web service. It is the most often attacked web-server platform on the Internet today. As a result, it has had the most bugs found, and the most flaws exploited. This server is not installed by default, but should not exist on your average workstation. If it is not going to be properly maintained by personnel with an education in IIS security, it should be disabled or removed.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > "Services.msc" and view the W3SVC status.

Remediation: If this service exists, disable it by stopping it and setting startup type to manual.

4.1.42 Data Execution Prevention

Description: Data Execution Prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help prevent malicious code from running on a system. In Microsoft Windows XP Service Pack 2 (SP2) and Microsoft Windows XP Tablet PC Edition 2005, DEP is enforced by hardware and by software.

The primary benefit of DEP is to help prevent code execution from data pages. Typically, code is not executed from the default heap and the stack. Hardware-enforced DEP detects code that is running from these locations and raises an exception when execution occurs. Software-enforced DEP can help prevent malicious code from taking advantage of exception-handling mechanisms in Windows. There are four settings for how DEP is configured:

OptIn **-** This setting is the default configuration. On systems with processors that can implement hardware-enforced DEP, DEP is enabled by default for limited system binaries and programs that "opt-in." With this option, only Windows system binaries are covered by DEP by default.

OptOut **-** DEP is enabled by default for all processes. You can manually create a list of specific programs that do not have DEP applied by using the **System** dialog box in Control Panel. Information technology (IT) professionals can use the Application Compatibility Toolkit to "opt-out" one or more programs from DEP protection. System compatibility fixes, or shims, for DEP do take effect.

AlwaysOn **-** This setting provides full DEP coverage for the whole system. All processes always run with DEP applied. The exceptions list to exempt specific programs from DEP protection is not available. System compatibility fixes for DEP do not take effect. Programs that have been opted-out by using the Application Compatibility Toolkit run with DEP applied.

AlwaysOff - **t**his setting does not provide any DEP coverage for any part of the system, regardless of hardware DEP support. The processor does not run in PAE mode unless the **/PAE** option is present in the Boot.ini file.

Recommendation Level: 1

Scoring Status: Scorable.

Audit: Start > Run > “sysdm.cpl”>Advanced tab under performance click settings and view the “Data Execution Prevention” tab.

Remediation:
If you are logged on as an administrator, you can manually configure DEP to switch between the OptIn and OptOut policies by using the **Data Execution Prevention** tab in **System Properties**. The following procedure describes how to manually configure DEP on the computer:

1. Click **Start**, click **Run**, type sysdm.cpl, and then click **OK**.
2. On the **Advanced** tab, under **Performance**, click **Settings**.
3. On the **Data Execution Prevention** tab, use one of the following procedures:
    - Click **Turn on DEP for essential Windows programs and services only** to select the OptIn policy.

- Click **Turn on DEP for all programs and services except those I select** to select the OptOut policy, and then click **Add** to add the programs that you do not want to use the DEP feature.

4. Click **OK** two times.

Reference: http://support.microsoft.com/kb/875352

4.2 User Rights

A number of individual rights can be assigned to users or groups to grant abilities beyond the reach of normal users. Some rights apply to domain controllers only.

User rights policies must be considered along with audit policy to protect the confidentiality and availability of resources. Often an application will not perform properly when user rights are configured. Rather than running the application with full administrative rights, the audit policy will allow a system administrator to examine logs for audit failures, and identify exactly which privileges are required by the application. Event logs typically refer to the privilege name (e.g., SeNetworkLogonRight) and not the actual description.

To complete the Audit and Remediation steps in the following section please download the NTRIGHTS utility which you can get from the Windows Server 2003 Resource Kit.

4.2.1 Access this computer from the network (SeNetworkLogonRight)

The ability to access a computer from the network is a user right that can be granted or revoked on any machine as appropriate. If this list is left empty, no user accounts can be used to gain access to the resources of this computer from the network.

4.2.2 Act as part of the operating system (SeTcbPrivilege)

The operating system works in a special security context called “Local System”. This security context has the ability to do things which normal users and administrative users can not. Granting this user right to users or groups will give them the ability to exceed normal privilege, regardless of their group membership.

4.2.3 Add workstations to domain (SeMachineAccountPrivilege)

By granting this right to a user account, the account will be allowed to add ten computers to the domain. The user receives an error when adding the eleventh computer, and the action fails. In order to add an unlimited number of machines to the domain, grant users the “Create Computer Accounts” right for an Organizational Unit in Active Directory.

4.2.4 Adjust memory quotas for a process (SeIncreaseQuotaPrivilege)

This policy setting defines the accounts which can adjust the maximum amount of memory assigned to a process.

4.2.5 Allow logon locally (SeInteractiveLogonRight)

Anyone who logs on locally to a computer must be listed here, either by individual user names, or by the “users” group.

4.2.6 Allow logon Through Terminal Services (SeRemoteInteractiveLogonRight)

If terminal services are enabled, use this setting to explicitly control which users are allowed to remotely access the workstation.

4.2.7 Back up files and directories (SeBackupPrivilege)

This user right grants a user or group the ability to circumvent normal Windows file security for the purposes of backing up files and folders. An account with this right will be granted read access to any file regardless of the file’s access control list. It should be restricted when possible.

4.2.8 Bypass traverse checking (SeChangeNotifyPrivilege)

The Bypassing Traverse Checking user right allows access to files or folders regardless of the user’s permissions to the parent folder. In other words, prevents the inheritance of permissions. Unfortunately, it is necessary to grant this right to users to allow normal operation of applications on a workstation. This right also allows the account to receive notification of file & directory changes.

4.2.9 Change the system time (SeSystemTimePrivilege)

Should a user change the time on a system, all future logging would reflect the new time. The time change event would be noted in the event logs; however, a time change event would be confusing for other logs such as IIS web and FTP logs. This should not be configurable to anyone except Administrators.

4.2.10 Create a pagefile (SeCreatePagefilePrivilege)

In order to protect the potentially sensitive information that can be stored in a pagefile, the creation of pagefiles should be restricted to Administrators.

4.2.11 Create a token object (SeCreateTokenPrivilege)

This right allows the creation of a security access token. Process requiring this right should be running under the Local System account. This right should never be given to any user.

4.2.12 Create global objects (SeCreateGlobalPrivilege)

Global objects are accessible to all processes running on the system. Any user able to create global objects could impact all processes running on the computer.

4.2.13 Create permanent shared objects (SeCreatePermanentPrivilege)

The right to create permanent shared objects should only be used by applications in the Windows kernel. The kernel already has the right to create such objects, so no users should ever be granted this right.

4.2.14 Debug programs (SeDebugPrivilege)

Any user can debug his or her programs, but this right allows a user to debug other processes on a machine. Users should not be granted this right except in an isolated development environment.

The SeDebugPrivilege raises a particular security concern. It should only be granted when absolutely necessary, and additional precautions may be necessary. This privilege allows the account to gain access to the Local Security Authority (LSA), which holds the machine secrets. Multiple exploits of this right exist which reap accounts, passwords and other secrets from protected locations in the registry. If it is necessary to grant this right, limit it to as few accounts and machines as possible; consider strengthening account logon and cached account settings on affected computers to reduce the exposure.

4.2.15 Deny access to this computer from the network (SeDenyNetworkLogonRight)

The “Deny Access” user rights always supercede the “Allow Access” user rights, so that if a user is listed under both user rights, that user will be denied access. If there are no users who should be allowed access to a computer from the network, the Everyone group should be listed in the “Deny Access to this computer from the network” user right.

This right manages network protocols which authenticate using Microsoft protocols. However, it obviously will not affect unauthenticated protocols (e.g., small services), and may not affect custom applications that do not enforce this right.

4.2.16 Deny logon as a batch job (SeDenyBatchLogonRight)

Just like the other “Deny…” user rights, a user listed here will be denied access to logon as a batch job, even if he has been explicitly granted that right.

4.2.17 Deny logon as a service (SeDenyBatchLogonRight)

Just like the other “Deny…” user rights, a user listed here will be denied access to logon as a service, even if he has been explicitly granted that right.

4.2.18 Deny logon locally (SeDenyInteractiveLogonRight)

Just like the other “Deny…” user rights, a user listed here will be denied access to logon to the console, even if he has been explicitly granted that right.

4.2.19 Deny log on Through Terminal Services (SeDenyRemoteInteractiveLogonRight)

Similar to the other “Deny…” rights, groups and accounts in this list will not be able to connect to the workstation using terminal services.

4.2.20 Enable computer and user accounts to be trusted for delegation (SeEnableDelegationPrivilege)

When a user is granted this right, they are able to change the “trusted for delegation” setting on other domain accounts. Misuse of this right could lead to impersonation attacks through the Kerberos authentication protocol.

This setting only affects domain controllers, and should not be assigned to other servers or workstations.

4.2.21 Force shutdown from a remote system (SeRemoteShutdownPrivilege)

This grants a user the right to shut down a computer from the network. It should only be granted to Administrators, and may be restricted to no users or groups at all.

4.2.22 Generate security audits (SeAuditPrivilege)

This user right allows a user or process to generate events to be added to the Windows Security Event Log.

4.2.23 Impersonate a client after authentication (SeImpersonatePrivilege)

This right will typically be granted to a service account so it can pass the client authentication on to another service. When using the service, a client will present a Kerberos ticket to gain access. The service can then present the ticket to other services on behalf of the client; the additional services then understand they are acting on behalf of the client.

For example, consider a three-tier (client / application / data) system. The client authenticates to the application by presenting a service ticket for the application. When the application requests data from the database server, it can present the client’s ticket to the database. The database then understands that it is serving data to the client, and can control the data and log accordingly.

4.2.24 Increase scheduling priority (SeIncreaseBasePriorityPrivilege)

The scheduling priority is one of the settings that can be altered as needed for performance tuning, but normal users should not have the ability to change the priority of other processes.

4.2.25 Load and unload device drivers (SeLoadDriverPrivilege)

Device drivers execute as highly privileged applications on a Windows computer because they directly interface the hardware with the operating system. These drivers can be the source of “Trojan Horse” applications, and should be restricted where possible. This setting actually applies to the installation of Plug and Play device drivers.

4.2.26 Lock pages in memory (SeLockMemoryPrivilege)

The right to lock pages in memory is the ability to force data in physical memory to remain in physical memory, and not be paged to disk, which can seriously degrade system performance. This user right is obsolete, and should remain empty.

4.2.27 Log on as a batch job (SeBatchLogonRight)

The right to log on as a batch job means that the listed user has the ability to log on using the batch queue facility. By default, Administrators have this right, but very rarely use it. Remove all users and groups from this right.

4.2.28 Log on as a service (SeServiceLogonRight)

Most applications that do not directly interact with the logged on user (and many that do) actually operate as a service. These services almost always execute under the Local System security credentials. If a service needs to be executed in a user context, that user would have to be listed here.

4.2.29 Manage auditing and security log (SeSecurityPrivilege)

The ability to manage the security event log is the equivalent to the ability for an intruder to cover his tracks and destroy evidence of what has been done to a computer system. This user right should be highly restricted, possibly even to only a subset of system administrators.

4.2.30 Modify firmware environment values (SeSystemEnvironmentPrivilege)

For systems with nonvolatile RAM, accounts with this privilege have the ability to modify that memory.

4.2.31 Perform Volume Maintenance Tasks (SeManageVolumePrivilege)

The most common volume maintenance tasks are defrag and chkdsk. In addition to the potential performance impact, this right could also allow low-level access to files bypassing standard permission constraints.

4.2.32 Profile single process (SeProfileSingleProcessPrivilege)

This user right grants the ability for one user to monitor the performance of another user or non-system process.

4.2.33 Profile system performance (SeSystemProfilePrivilege)

The Profile system performance user right allows a user or group of users to monitor system performance, including system processes.

4.2.34 Remove computer from docking station (SeUndockPrivilege)

This user right allows the user to select “Eject PC” from the Start menu.

4.2.35 Replace a process level token (SeAssignPrimaryTokenPrivilege)

The ability to replace a process level token essentially means that a process can change the authentication authority of its own child-processes.

4.2.36 Restore files and directories (SeRestorePrivilege)

In conjunction with the “Backup files and directories” user right, this can be very dangerous if a user backs up certain security related information, alters it, and restores it back to the same place. Accounts with this privilege have right access to all files, regardless of the file’s access control list. It should be restricted to Administrators.

4.2.37 Shut down the system (SeShutdownPrivilege)

Users granted this right will have the ability to shut down the computer. This only takes effect if users are required to log on to shut down a system.

4.2.38 Synchronize directory service data (SeSynchAgentPrivilege)

This right allows the account to read all the data in Active Directory in order to perform synchronization. Only the System account on domain controllers should have this right.

4.2.39 Take ownership of files or other objects (SeTakeOwnershipPrivilege)

A user who “owns” a file has greater authority over that file than even the permissions would suggest. The right to take ownership of a file is equivalent to the ability to compromise an entire file system.

4.3 Other System Requirements

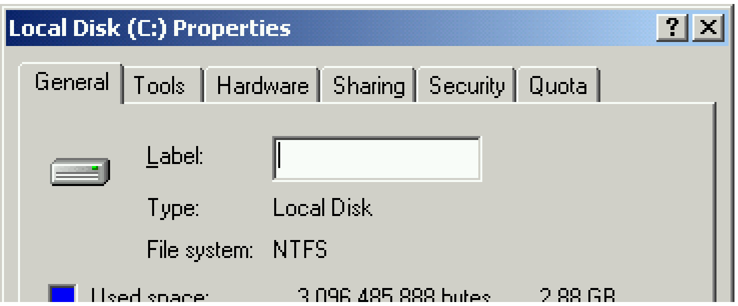
4.3.1 Ensure all disk volumes are using the NTFS file system

Warning: Do not do this if your system is a dual-boot system with Windows 95/98/Me. The alternate operating system will cease to function, and can not be recovered.

Since the early days of DOS, files have been stored on floppy disks. These disks break up data into blocks, and those blocks are written to similar blocks on a physical disk. The “map” describing which blocks are holding which files is stored on part of the disk called the “File Allocation Table” or FAT. When DOS moved to Hard Disks, the same FAT style of disk allocation was used. FAT filesystems had some good points – most of all, it’s pretty simple. Any system could read the disks, and if there was a problem, the data could have been restored. When disks began to grow beyond the size of FAT’s capabilities, it was expanded to FAT32, allowing for larger disks. However, FAT and FAT32 do not offer any security.

NTFS interoperability has come a long way since its initial introduction. It can be bypassed if the system can be rebooted, but it is the ONLY way that any file-level security can be enforced while system is operating.

To determine if a disk volume is NTFS, double click “My Computer” on the desktop. Right-click the C drive (C:) and click Properties. The properties pane for that disk will describe the “File System” as either FAT or NTFS.



Label:

Type: Local Disk

File system: NTFS

Used space: 3,096,485,888 bytes 2.88 GB

In order to make a FAT disk into an NTFS disk, open a Command Prompt (Click Start -> Programs -> Accessories -> Command Prompt) and type "Convert C: /fs:ntfs". The system will probably be required to restart to perform this task. Take the same action with the D: drive and any others that show up as FAT disks.

Once the disks have been converted to the NTFS file system, default security must be applied to the boot drive (C:). Open a command prompt (click Start, Programs, Accessories, and Command Prompt) and type the following command for workstations:

"secedit /configure /db default.sdb /cfg %windir%\inf\defltwk.inf /areas filestore"

or the following command for servers:

"secedit /configure /db default.sdb /cfg %windir%\inf\defltsv.inf /areas filestore"

and press enter. The /db parameter is required, even though the database does not exist until after the command is run. Type "secedit /?" for more information on this command.

Other applications will have the ability to use these security features. Most users never need to update these file permissions, while system administrators of all levels will need to do so from time to time. In fact, it is possible to cripple a system by incorrectly modifying that security. It is important to keep in mind that this is still a step up from a FAT filesystem with NO security. An important point here is that for maximum security you should have no other FAT filesystem partitions on disk as is sometimes done with separate boot and data partitions.

4.3.2 Disable NetBIOS

Windows 2000 introduced the ability to eliminate NetBIOS and WINS for locating resources, in favor of a direct TCP connection through DNS.

Disabling NetBIOS reduces the services running on the workstation. The NetBIOS name service runs on TCP and UDP port 137, the datagram service listens on UDP port 138 and the session service listens on TCP port 139. All SMB resource sharing applications will use TCP and UDP port 445, and ports 137, 138 and 139 can be firewalled.

NetBIOS can only effectively be disabled if all shared resources on the client network run on Windows 2000 or later.

See Microsoft Knowledge Base article 299977 for additional items to consider when disabling NetBIOS. Also see Knowledge Base article 315267 for information on how to disable NetBIOS on Windows XP.

Warning: Disabling NetBIOS is NOT supported by Microsoft and can result in loss of functionality and unstable/unpredictable system behavior. Proper testing should be conducted on **non-production** systems to determine the impact of disabling NetBIOS on your systems/networks.

4.3.3 Enable the Internet Connection Firewall

In general, the Windows Firewall is available only when you are connected directly to the Internet, but not for Local Area Network (LAN) connections. The firewall is also enabled on dial-up Internet connections and shared Internet connections.

When enabled, the Windows Firewall blocks inbound traffic to your workstation unless a port is explicitly opened. The Windows Firewall typically is not necessary on internal networks where a firewall already exists between the client and the untrusted network. The Windows Firewall also supports activity logging.

For more information about the Windows Firewall on Windows XP, see Microsoft Knowledge Base Article 320855.

4.3.4 Restricted Groups

With Restricted Groups enabled, the operating system will evaluate local group membership on boot and when group policy refreshes. Members in the "Restricted Groups" policy are compared against the actual, current group membership. If the accounts listed in the policy are not in the group, they are added. Conversely, if an account is in the group but not in the policy, it is removed.

4.3.5 Antivirus software present

Most servers need some antivirus protection to protect from any virii that originate from a website or email received by a user on the server or from a workstation on the network that is already infected. It is more then likely that you need some antivirus on your server but keep in mind this does increase the attack surface. To help mitigate any vulnerabilities found and to keep the antivirus software relevant and useful be sure to keep the antivirus software up to date.

4.4 File and Registry Permissions

Once a volume has been converted to NTFS, and once the basic file security settings have been applied, additional settings should be applied. Most known operating system and application exploits exist because of multiple factors. First, there is an application that has a flaw that opens a low-privileged door into an operating system. And second, that open door allows a knowledgeable intruder to elevate his privilege and take over the system. The permissions listed below will help to make an operating system "resistant" to privilege elevation, even to potential software vulnerabilities that have not yet been discovered.

WARNING: It is possible that the permissions applied here can take away some sort of application functionality that you are accustomed to. If that happens and you need to back off to a previously known state, use the same instructions that were used to apply the basic permissions to a freshly converted NTFS file system to "undo" most of the settings you see below.

4.4.1 File Permissions

File permissions are used to limit access to sensitive programs. Often file permissions provide a final layer of protection to prevent an attacker from gaining or elevating access on the system.

4.4.2 Registry Permissions

The registry contains many sensitive settings which control the behavior of almost all aspects of the system and its applications. The operating system allows specific access controls to be placed on each registry folder, similar to permissions on file folders.

Item 4.4.2.5: When running the CIS NG Scoring Tool, this test will fail with two "Access denied to key" errors with the default permission set on the HKLM\CurrentControlSet\Enum key. Application of the CIS recommended registry key permissions will allow this key to be successfully inspected by the scoring tool without errors.

Item 4.4.2.10: When running the CIS NG Scoring Tool, this test will fail with two "Access denied to key" errors with the default permissions set on the HKLM\Default\Software\Microsoft\SystemCertificates\Root\ProtectedRoots key. Application of the CIS recommended registry key permissions will allow this key to be successfully inspected by the scoring tool without errors.

4.4.3 File and Registry Auditing

A valuable tool that is available to NTFS volumes, in addition to NTFS Permissions, is the ability to audit what exactly happens to files on a file system. You can audit – user by user, when a file is accessed, modified, or created. The benefit of security auditing after a system has been compromised can be incredible – if auditing was actually turned on before the compromise, you can get a play-by-play description of exactly what happened, and what files were viewed or modified by each user. If auditing is not enabled before the compromise, there is no information to audit.

This feature of NTFS file systems is not normally used because there is a level of performance overhead involved, and because the security audit log will tend to be flooded with events. We've already dealt with the event log by significantly increasing its size. The performance overhead is something that users are likely to notice; especially during computer start-up and shut-down.

The ability to audit accesses and changes to the file system is also extended to the system registry. You can enable auditing for different registry hives, keys, and values as well. It is necessary to monitor changes to the registry as well as the file system to track what has been compromised on a computer.

Appendix A: Internet Resources

The Center for Internet Security – http://www.cisecurity.org

The SANS Institute – http://www.sans.org

National Security Agency Security Recommendation Guides – http://nsa1.www.conxion.com

Department of Defense recommendations – not currently available online.

Microsoft Windows Security – http://www.microsoft.com/security
Windows XP Security Guide – http://go.microsoft.com/fwlink/?LinkId=14839
Server 2003 Security Guide – http://go.microsoft.com/fwlink/?LinkId=14845
Threats and Countermeasures Guide – http://go.microsoft.com/fwlink/?LinkId=15159

Microsoft Directory Services Client for Windows 9x/Me - http://www.microsoft.com/technet/prodtechnol/ntwrkstn/downloads/utils/dsclient.mspx

The CIS Scoring Tool that accompanies this document uses the Microsoft Network Security Hotfix Checker (HfNetChk), which is licensed to Microsoft by Shavlik Technologies – http://www.shavlik.com/

Windows NT Magazine article regarding editing the Registry - http://www.microsoft.com/technet/prodtechnol/winntas/tips/winntmag/inreg.mspx

Appendix B: New To Windows 2003

- User Rights
  - Impersonate a client after authentication (SeImpersonatePrivilege)
- Security Settings
  - Network access: Remotely accessible registry paths and subpaths
  - Network access: Restrict anonymous access to Named Pipes and Shares
  - System cryptography: Force strong key protection for user keys stored on the computer
  - System settings: Optional subsystems
  - System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies
- Services
  - Application Layer Gateway Service (ALG)
  - Application Management (AppMgmt)
  - ASP .NET State Service (aspnet_state)
  - Cluster Service (ClusSvc)
  - Cyrptographic Services (CryptSvc)
  - HTTP SSL (HTTPFilter)
  - IAS Jet Database Access (IASJet)
  - IMAPI CD-Burning COM Service (ImapiService)
  - IP Version 6 Helper Service (6to4)
  - MS Software Shadow Copy Provider (SwPrv)
  - MSSQL$UDDI (MSSQL$UDDI)
  - MSSQLServerADHelper (MSSQLServerADHelper)
  - .NET Framework Support Service (CORRTSvc)
  - Remote Administration Service (SrvcSurg)
  - Remote Installation (BINLSVC)
  - Remote Server Manager (AppMgr)
  - Remote Server Monitor (Appmon)
  - Remote Storage Notification (Remote_Storage_User_Link)
  - Remote Storage Server (Remote_Storage_Server)
  - Resultant Set of Policy Provider (RSoPProv)
  - Single Instance Storage Groveler (Groveler)
  - Special Administration Console Helper (Sacsvr)
  - SQLAgent$* (* UDDI or WebDB) (SQLAgent$WEBDB)
  - TCP/IP Print Server (LPDSVC)
  - Trivial FTP Daemon (tftpd)
  - Upload Manager (Uploadmgr)
  - Virtual Disk Service (VDS)
  - Volume Shadow Copy (VSS)
  - Web Element Manager (elementmgr)
  - Windows Audio (AudioSrv)
  - Windows System Resource Manager (WindowsSystemResourceManager)

Appendix C: Change History

September 3, 2004 – Version 1.0 released to public.

October 14, 2004 – Version 1.0.2
Corrected document value of 3.2.1.67 MSS: AFD MaximumDynamicBacklog from 2000 to 20000. Templates are unaffected.

October 20, 2004 – Version 1.1
Renamed "High Security" to "Specialized Security – Limited Functionality"

October 18, 2005 – Version 1.2

- Corrected numbering errors in section 2 of the benchmark so that they correctly reflect numbering in section 1.
- Altered descriptive text in several sections for accuracy and completeness.
- No recommendations were added nor were any recommended values altered.

October 1-November, 2007 – Version 1.3

- Reformatted document to be more in line with the style guide.
- Added limited new information about SP1 and SP2
- Altered descriptive text in several sections for accuracy and completeness.

Appendix D: Known Application Exceptions

This is a list of known application incompatibilities. It is not all-inclusive, and any additions can be submitted to windows-feedback@cisecurity.org.

Exchange Server 2003 – User rights "Access this computer from the network" and "Deny access to this computer from the network" must be modified to allow "Guests" and "Anonymous Logon" to access the computer from the network in order for aspects of Exchange Server 2003 to function properly.

Appendix E: Modifying your sceregvl.inf

1. Navigate to %systemroot%\inf which will most likely be C:\windows\inf
2. Open sceregvl.inf in notepad.
3. Replace sceregvl.inf with the one listed below.
4. Open a cmd.exe window and type "regsvr32 scecli.dll."
5. Ensure that regsvr32 successfully registered.

```
; Copyright (c) Microsoft Corporation.  All rights reserved.
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name:        SCERegVl.INF
; Template Version:     05.00.DR.0000
;
; Revision History
; 0000  -       Original

[version]
signature="$CHICAGO$"
DriverVer=10/01/2002,5.2.3790.0

[Register Registry Values]
;
; Syntax: RegPath,RegType,DisplayName,DisplayType,Options
; where
;         RegPath:      Includes the registry keypath and value
;         RegType:      1 - REG_SZ, 2 - REG_EXPAND_SZ, 3 - REG_BINARY, 
4 - REG_DWORD, 7 - REG_MULTI_SZ
;         Display Name: Is a localizable string defined in the 
[strings] section
;         Display type: 0 - boolean, 1 - Number, 2 - String, 3 - 
Choices, 4 - Multivalued, 5 - Bitmask
;         Options:      If Displaytype is 3 (Choices) or 5 (Bitmask), 
then specify the range of values and corresponding display strings
;                       in value|displaystring format separated by a 
comma.


MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects,4,%AuditB
aseObjects%,0
```

```
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail,4,%CrashO
nAuditFail%,0
MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds,4,%Disa
bleDomainCreds%,0
MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous,
4,%EveryoneIncludesAnonymous%,0
MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest,4,%ForceGuest%,
3,0|%Classic%,1|%GuestBased%
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing,3,%F
ullPrivilegeAuditing%,0
MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse,4,%L
imitBlankPasswordUse%,0
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel,4,%Lm
CompatibilityLevel%,3,0|%LMCLevel0%,1|%LMCLevel1%,2|%LMCLevel2%,3|%LMCL
evel3%,4|%LMCLevel4%,5|%LMCLevel5%
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec,4,
%NTLMMinClientSec%,5,16|%NTLMIntegrity%,32|%NTLMConfidentiality%,524288
|%NTLMv2Session%,536870912|%NTLM128%
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec,4,
%NTLMMinServerSec%,5,16|%NTLMIntegrity%,32|%NTLMConfidentiality%,524288
|%NTLMv2Session%,536870912|%NTLM128%
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash,4,%NoLMHash%,0
MACHINE\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner,4,%NoD
efaultAdminOwner%,3,0|%DefaultOwner0%,1|%DefaultOwner1%
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous,4,%Restr
ictAnonymous%,0
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM,4,%Re
strictAnonymousSAM%,0
MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl,4,%SubmitCon
trol%,0
MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy,4,%FIP
S%,0

MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers,4,%AddPrintDrivers%,0

MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\Allow
edPaths\Machine,7,%AllowedPaths%,4
MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\Allow
edExactPaths\Machine,7,%AllowedExactPaths%,4

MACHINE\System\CurrentControlSet\Control\Session
Manager\Kernel\ObCaseInsensitive,4,%ObCaseInsensitive%,0
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown,4,%ClearPageFileAtShutdown%,0
MACHINE\System\CurrentControlSet\Control\Session
Manager\ProtectionMode,4,%ProtectionMode%,0
MACHINE\System\CurrentControlSet\Control\Session
Manager\SubSystems\optional,7,%OptionalSubSystems%,4

MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\Enabl
eSecuritySignature,4,%EnableSMBSignServer%,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\Requi
reSecuritySignature,4,%RequireSMBSignServer%,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\Enabl
eForcedLogOff,4,%EnableForcedLogoff%,0
```

```
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoD
isconnect,4,%AutoDisconnect%,1,%Unit-Minutes%
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\Restr
ictNullSessAccess,4,%RestrictNullSessAccess%,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullS
essionPipes,7,%NullPipes%,4
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullS
essionShares,7,%NullShares%,4

MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\
EnableSecuritySignature,4,%EnableSMBSignRDR%,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\
RequireSecuritySignature,4,%RequireSMBSignRDR%,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\
EnablePlainTextPassword,4,%EnablePlainTextPassword%,0

MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity,4,%L
DAPClientIntegrity%,3,0|%LDAPClient0%,1|%LDAPClient1%,2|%LDAPClient2%

MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePa
sswordChange,4,%DisablePWChange%,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPa
sswordAge,4,%MaximumPWAge%,1,%Unit-Days%
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RefusePas
swordChange,4,%RefusePWChange%,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecur
eChannel,4,%SignSecureChannel%,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecur
eChannel,4,%SealSecureChannel%,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSi
gnOrSeal,4,%SignOrSeal%,0
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSt
rongKey,4,%StrongKey%,1

MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerInt
egrity,4,%LDAPServerIntegrity%,3,1|%LDAPServer1%,2|%LDAPServer2%

MACHINE\Software\Microsoft\Driver
Signing\Policy,3,%DriverSigning%,3,0|%DriverSigning0%,1|%DriverSigning1
%,2|%DriverSigning2%

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Disab
leCAD,4,%DisableCAD%,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontD
isplayLastUserName,4,%DontDisplayLastUserName%,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Legal
NoticeCaption,1,%LegalNoticeCaption%,2
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Legal
NoticeText,7,%LegalNoticeText%,4
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ScFor
ceOption,4,%ScForceOption%,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shutd
ownWithoutLogon,4,%ShutdownWithoutLogon%,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\Undoc
kWithoutLogon,4,%UndockWithoutLogon%,0
```

```
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel,4,%RCAdmin%,0
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Setup\RecoveryConsole\SetCommand,4,%RCSet%,0

MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\AllocateCDRoms,1,%AllocateCDRoms%,0
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\AllocateDASD,1,%AllocateDASD%,3,0|%AllocateD
ASD0%,1|%AllocateDASD1%,2|%AllocateDASD2%
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\AllocateFloppies,1,%AllocateFloppies%,0
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\CachedLogonsCount,1,%CachedLogonsCount%,1,%U
nit-Logons%
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ForceUnlockLogon,4,%ForceUnlockLogon%,0
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\PasswordExpiryWarning,4,%PasswordExpiryWarni
ng%,1,%Unit-Days%
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ScRemoveOption,1,%ScRemove%,3,0|%ScRemove0%,
1|%ScRemove1%,2|%ScRemove2%

MACHINE\Software\Policies\Microsoft\Cryptography\ForceKeyProtection,4,%
ForceHighProtection%,3,0|%CryptAllowNoUI%,1|%CryptAllowNoPass%,2|%Crypt
UsePass%
MACHINE\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\Authe
nticodeEnabled,4,%AuthenticodeEnabled%,0

; delete these values from the UI - Rdr in case NT4 w SCE
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\DisableCAD
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\DontDisplayLastUserName
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\LegalNoticeCaption
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\LegalNoticeText
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ShutdownWithoutLogon
MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\CmdConsSecurityLevel
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\AddPrintDrivers
MACHINE\System\CurrentControlSet\Services\MRxSMB\Parameters\EnableSecur
itySignature
MACHINE\System\CurrentControlSet\Services\MRxSMB\Parameters\RequireSecu
ritySignature
MACHINE\System\CurrentControlSet\Services\MRxSMB\Parameters\EnablePlain
TextPassword
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnableSecurity
Signature
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\RequireSecurit
ySignature
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnablePlainTex
tPassword
```

```
MACHINE\Software\Microsoft\Windows\CurrentVersion\NetCache\EncryptEntir
eCache
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\EFS\AlgorithmID
MACHINE\Software\Microsoft\Non-Driver Signing\Policy
MACHINE\Software\Policies\Microsoft\Cryptography\ForceHighProtection


;================================= MSS Values
=================================
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRe
direct,4,%EnableICMPRedirect%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackPro
tect,4,%SynAttackProtect%,3,0|%SynAttackProtect0%,1|%SynAttackProtect1%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGW
Detect,4,%EnableDeadGWDetect%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDi
scovery,4,%EnablePMTUDiscovery%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTim
e,4,%KeepAliveTime%,3,150000|%KeepAliveTime0%,300000|%KeepAliveTime1%,6
00000|%KeepAliveTime2%,1200000|%KeepAliveTime3%,2400000|%KeepAliveTime4
%,3600000|%KeepAliveTime5%,7200000|%KeepAliveTime6%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSou
rceRouting,4,%DisableIPSourceRouting%,3,0|%DisableIPSourceRouting0%,1|%
DisableIPSourceRouting1%,2|%DisableIPSourceRouting2%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnec
tResponseRetransmissions,4,%TcpMaxConnectResponseRetransmissions%,3,0|%
TcpMaxConnectResponseRetransmissions0%,1|%TcpMaxConnectResponseRetransm
issions1%,2|%TcpMaxConnectResponseRetransmissions2%,3|%TcpMaxConnectRes
ponseRetransmissions3%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRe
transmissions,4,%TcpMaxDataRetransmissions%,1
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRoute
rDiscovery,4,%PerformRouterDiscovery%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TCPMaxPortsE
xhausted,4,%TCPMaxPortsExhausted%,1
MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleas
eOnDemand,4,%NoNameReleaseOnDemand%,0
MACHINE\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3Nam
eCreation,4,%NtfsDisable8dot3NameCreation%,0
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoD
riveTypeAutoRun,4,%NoDriveTypeAutoRun%,3,0|%NoDriveTypeAutoRun0%,255|%N
oDriveTypeAutoRun1%
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLeve
l,4,%WarningLevel%,3,50|%WarningLevel0%,60|%WarningLevel1%,70|%WarningL
evel2%,80|%WarningLevel3%,90|%WarningLevel4%
MACHINE\SYSTEM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod,4,%ScreenSaverGracePe
riod%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\DynamicBacklog
GrowthDelta,4,%DynamicBacklogGrowthDelta%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\EnableDynamicB
acklog,4,%EnableDynamicBacklog%,0
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\MinimumDynamic
Backlog,4,%MinimumDynamicBacklog%,1
MACHINE\System\CurrentControlSet\Services\AFD\Parameters\MaximumDynamic
Backlog,4,%MaximumDynamicBacklog%,3,10000|%MaximumDynamicBacklog0%,1500
0|%MaximumDynamicBacklog1%,20000|%MaximumDynamicBacklog2%,40000|%Maximu
```

```
mDynamicBacklog3%,80000|%MaximumDynamicBacklog4%,160000|%MaximumDynamic
Backlog5%
MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\SafeDllSearchMode,4,%SafeDllSearchMode%,0
```

```
[Strings]

;================================ Accounts
=======================================================================
=====
;Specified in UI code - Accounts: Administrator account status
;Specified in UI code - Accounts: Guest account status
;Specified in UI code - Accounts: Rename administrator account
;Specified in UI code - Accounts: Rename guest account
LimitBlankPasswordUse = "Accounts: Limit local account use of blank
passwords to console logon only"


;================================ Audit
=======================================================================
========
AuditBaseObjects="Audit: Audit the access of global system objects"
FullPrivilegeAuditing="Audit: Audit the use of Backup and Restore
privilege"
CrashOnAuditFail="Audit: Shut down system immediately if unable to log
security audits"
```

```
;================================ Devices
=======================================================================
======
AllocateDASD="Devices: Allowed to format and eject removable media"
AllocateDASD0="Administrators"
AllocateDASD1="Administrators and Power Users"
AllocateDASD2="Administrators and Interactive Users"
AddPrintDrivers="Devices: Prevent users from installing printer
drivers"
AllocateCDRoms="Devices: Restrict CD-ROM access to locally logged-on
user only"
AllocateFloppies="Devices: Restrict floppy access to locally logged-on
user only"
DriverSigning="Devices: Unsigned driver installation behavior"
DriverSigning0="Silently succeed "
DriverSigning1="Warn but allow installation"
DriverSigning2="Do not allow installation"
UndockWithoutLogon="Devices: Allow undock without having to log on"

;================================ Domain controller
====================================================================
SubmitControl="Domain controller: Allow server operators to schedule
tasks"
RefusePWChange="Domain controller: Refuse machine account password
changes"
LDAPServerIntegrity = "Domain controller: LDAP server signing
requirements"
LDAPServer1 = "None"
LDAPServer2 = "Require signing"

;================================ Domain member
=======================================================================
=
DisablePWChange="Domain member: Disable machine account password
changes"
MaximumPWAge="Domain member: Maximum machine account password age"
SignOrSeal="Domain member: Digitally encrypt or sign secure channel
data (always)"
SealSecureChannel="Domain member: Digitally encrypt secure channel data
(when possible)"
SignSecureChannel="Domain member: Digitally sign secure channel data
(when possible)"
StrongKey="Domain member: Require strong (Windows 2000 or later)
session key"

;================================ Interactive logon
====================================================================
DisableCAD = "Interactive logon: Do not require CTRL+ALT+DEL"
DontDisplayLastUserName = "Interactive logon: Do not display last user
name"
LegalNoticeText = "Interactive logon: Message text for users attempting
to log on"
LegalNoticeCaption = "Interactive logon: Message title for users
attempting to log on"
CachedLogonsCount = "Interactive logon: Number of previous logons to
cache (in case domain controller is not available)"
```

```
PasswordExpiryWarning = "Interactive logon: Prompt user to change
password before expiration"
ForceUnlockLogon = "Interactive logon: Require Domain Controller
authentication to unlock workstation"
ScForceOption = "Interactive logon: Require smart card"
ScRemove = "Interactive logon: Smart card removal behavior"
ScRemove0 = "No Action"
ScRemove1 = "Lock Workstation"
ScRemove2 = "Force Logoff"

;================================ Microsoft network client
=============================================================
RequireSMBSignRdr="Microsoft network client: Digitally sign
communications (always)"
EnableSMBSignRdr="Microsoft network client: Digitally sign
communications (if server agrees)"
EnablePlainTextPassword="Microsoft network client: Send unencrypted
password to third-party SMB servers"

;================================ Microsoft network server
=============================================================
AutoDisconnect="Microsoft network server: Amount of idle time required
before suspending session"
RequireSMBSignServer="Microsoft network server: Digitally sign
communications (always)"
EnableSMBSignServer="Microsoft network server: Digitally sign
communications (if client agrees)"
EnableForcedLogoff="Microsoft network server: Disconnect clients when
logon hours expire"

;================================ Network access
=======================================================================
;Specified in UI code - Network access: Allow anonymous SID/Name
translation
DisableDomainCreds = "Network access: Do not allow storage of
credentials or .NET Passports for network authentication"
RestrictAnonymousSAM = "Network access: Do not allow anonymous
enumeration of SAM accounts"
RestrictAnonymous = "Network access: Do not allow anonymous enumeration
of SAM accounts and shares"
EveryoneIncludesAnonymous = "Network access: Let Everyone permissions
apply to anonymous users"
RestrictNullSessAccess = "Network access: Restrict anonymous access to
Named Pipes and Shares"
NullPipes = "Network access: Named Pipes that can be accessed
anonymously"
NullShares = "Network access: Shares that can be accessed anonymously"
AllowedPaths = "Network access: Remotely accessible registry paths and
sub-paths"
AllowedExactPaths = "Network access: Remotely accessible registry
paths"
ForceGuest = "Network access: Sharing and security model for local
accounts"
Classic = "Classic - local users authenticate as themselves"
GuestBased = "Guest only - local users authenticate as Guest"
```

```
;================================ Network security
=====================================================================
;Specified in UI code - Network security: Enforce logon hour
restrictions
NoLMHash = "Network security: Do not store LAN Manager hash value on
next password change"
LmCompatibilityLevel = "Network security: LAN Manager authentication
level"
LMCLevel0 = "Send LM & NTLM responses"
LMCLevel1 = "Send LM & NTLM - use NTLMv2 session security if
negotiated"
LMCLevel2 = "Send NTLM response only"
LMCLevel3 = "Send NTLMv2 response only"
LMCLevel4 = "Send NTLMv2 response only\refuse LM"
LMCLevel5 = "Send NTLMv2 response only\refuse LM & NTLM"
NTLMMinClientSec = "Network security: Minimum session security for NTLM
SSP based (including secure RPC) clients"
NTLMMinServerSec = "Network security: Minimum session security for NTLM
SSP based (including secure RPC) servers"
NTLMIntegrity = "Require message integrity"
NTLMConfidentiality = "Require message confidentiality"
NTLMv2Session = "Require NTLMv2 session security"
NTLM128 = "Require 128-bit encryption"
LDAPClientIntegrity = "Network security: LDAP client signing
requirements"
LDAPClient0 = "None"
LDAPClient1 = "Negotiate signing"
LDAPClient2 = "Require signing"

;================================ Recovery console
====================================================================
RCAdmin="Recovery console: Allow automatic administrative logon"
RCSet="Recovery console: Allow floppy copy and access to all drives and
all folders"

;================================ Shutdown
=======================================================================
=====
ShutdownWithoutLogon="Shutdown: Allow system to be shut down without
having to log on"
ClearPageFileAtShutdown="Shutdown: Clear virtual memory pagefile"

ProtectionMode = "System objects: Strengthen default permissions of
internal system objects (e.g. Symbolic Links)"
NoDefaultAdminOwner = "System objects: Default owner for objects
created by members of the Administrators group"
DefaultOwner0 = "Administrators group"
DefaultOwner1 = "Object creator"
ObCaseInsensitive = "System objects: Require case insensitivity for
non-Windows subsystems"

;================================ System cryptography
=================================================================
FIPS="System cryptography: Use FIPS compliant algorithms for
encryption, hashing, and signing"
```

```
ForceHighProtection="System cryptography: Force strong key protection
for user keys stored on the computer"

CryptAllowNoUI="User input is not required when new keys are stored and
used"
CryptAllowNoPass="User is prompted when the key is first used"
CryptUsePass="User must enter a password each time they use a key"


;================================ System Settings
=====================================================================
AuthenticodeEnabled = "System settings: Use Certificate Rules on
Windows Executables for Software Restriction Policies"
OptionalSubSystems = "System settings: Optional subsystems"


Unit-Logons="logons"
Unit-Days="days"
Unit-Minutes="minutes"
Unit-Seconds="seconds"

;================================ MSS Settings
================================
EnableICMPRedirect = "MSS: (EnableICMPRedirect) Allow ICMP redirects to
override OSPF generated routes"
SynAttackProtect = "MSS: (SynAttackProtect) Syn attack protection level
(protects against DoS)"
SynAttackProtect0 = "No additional protection, use default settings"
SynAttackProtect1 = "Connections time out sooner if a SYN attack is
detected"
EnableDeadGWDetect = "MSS: (EnableDeadGWDetect) Allow automatic
detection of dead network gateways (could lead to DoS)"
EnablePMTUDiscovery = "MSS: (EnablePMTUDiscovery ) Allow automatic
detection of MTU size (possible DoS by an attacker using a small MTU)"
KeepAliveTime = "MSS: How often keep-alive packets are sent in
milliseconds"
KeepAliveTime0 ="150000 or 2.5 minutes"
KeepAliveTime1 ="300000 or 5 minutes (recommended)"
KeepAliveTime2 ="600000 or 10 minutes"
KeepAliveTime3 ="1200000 or 20 minutes"
KeepAliveTime4 ="2400000 or 40 minutes"
KeepAliveTime5 ="3600000 or 1 hour"
KeepAliveTime6 ="7200000 or 2 hours (default value)"
DisableIPSourceRouting = "MSS: (DisableIPSourceRouting) IP source
routing protection level (protects against packet spoofing)"
DisableIPSourceRouting0 = "No additional protection, source routed
packets are allowed"
DisableIPSourceRouting1 = "Medium, source routed packets ignored when
IP forwarding is enabled"
DisableIPSourceRouting2 = "Highest protection, source routing is
completely disabled"
TcpMaxConnectResponseRetransmissions = "MSS:
(TcpMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a
connection request is not acknowledged"
TcpMaxConnectResponseRetransmissions0 = "No retransmission, half-open
connections dropped after 3 seconds"
```

```
TcpMaxConnectResponseRetransmissions1 = "3 seconds, half-open
connections dropped after 9 seconds"
TcpMaxConnectResponseRetransmissions2 = "3 & 6 seconds, half-open
connections dropped after 21 seconds"
TcpMaxConnectResponseRetransmissions3 = "3, 6, & 9 seconds, half-open
connections dropped after 45 seconds"
TcpMaxDataRetransmissions = "MSS: (TcpMaxDataRetransmissions) How many
times unacknowledged data is retransmitted (3 recommended, 5 is
default)"
PerformRouterDiscovery = "MSS: (PerformRouterDiscovery) Allow IRDP to
detect and configure Default Gateway addresses (could lead to DoS)"
TCPMaxPortsExhausted = "MSS: (TCPMaxPortsExhausted) How many dropped
connect requests to initiate SYN attack protection (5 is recommended)"
NoNameReleaseOnDemand = "MSS: (NoNameReleaseOnDemand) Allow the
computer to ignore NetBIOS name release requests except from WINS
servers"
NtfsDisable8dot3NameCreation = "MSS: Enable the computer to stop
generating 8.3 style filenames"
NoDriveTypeAutoRun = "MSS: Disable Autorun for all drives"
NoDriveTypeAutoRun0 = "Null, allow Autorun"
NoDriveTypeAutoRun1 = "255, disable Autorun for all drives"
WarningLevel = "MSS: Percentage threshold for the security event log at
which the system will generate a warning"
WarningLevel0 = "50%"
WarningLevel1 = "60%"
WarningLevel2 = "70%"
WarningLevel3 = "80%"
WarningLevel4 = "90%"
ScreenSaverGracePeriod = "MSS: The time in seconds before the screen
saver grace period expires (0 recommended)"
DynamicBacklogGrowthDelta = "MSS: (AFD DynamicBacklogGrowthDelta)
Number of connections to create when additional connections are
necessary for Winsock applications (10 recommended)"
EnableDynamicBacklog = "MSS: (AFD EnableDynamicBacklog) Enable dynamic
backlog for Winsock applications (recommended)"
MinimumDynamicBacklog = "MSS: (AFD MinimumDynamicBacklog) Minimum
number of free connections for Winsock applications (20 recommended for
systems under attack, 10 otherwise)"
MaximumDynamicBacklog = "MSS: (AFD MaximumDynamicBacklog) Maximum
number of 'quasi-free' connections for Winsock applications"
MaximumDynamicBacklog0 = "10000"
MaximumDynamicBacklog1 = "15000"
MaximumDynamicBacklog2 = "20000 (recommended)"
MaximumDynamicBacklog3 = "40000"
MaximumDynamicBacklog4 = "80000"
MaximumDynamicBacklog5 = "160000"
SafeDllSearchMode = "MSS: Enable Safe DLL search mode (recommended)"
```