Windows 2000 Professional Operating System Level 2 Benchmark

Consensus Baseline Security Settings

Version 2.2.1

November 15, 2004

http://www.cisecurity.org

Editor: Jeff Shawgo

cis-feedback@cisecurity.org

Table of Contents

Agreed Terms of Use

Background.

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 and 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 any Product or Recommendation. 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 if it chooses at it sole option to do so; 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 and agree that we have read these Agreed Terms of Use in their entirety, understand them and 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 pendulum has been swinging 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 of the side-effects of the 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.

I want to run the tool now!

It is understandable to want to "hit the ground running". If you want to run the accompanying tool this very minute, go ahead and do so. Please look through the accompanying "Readme" file. The tool is designed to measure the status of your system against a minimum standard, and score it accordingly. The tool will not make changes to the security settings on your system, except that it must be installed as an application.

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 2000 professional compliant computer system. It is brief and to the point. 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 2000 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 2000 Professional Benchmark Consensus Baseline Security Settings

November 15, 2004

This document is a security benchmark for the Microsoft Windows 2000 Professional operating system for workstations. 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 2000 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 2000 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. If enough people become "Security Aware Users" then the safety level of the Internet will have improved dramatically.

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 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 hesitated to migrate to Active Directory because of the level of complexity involved. Once an infrastructure has been implemented to support an Active Directory domain, implementing most of these policies with Group Policy becomes relatively easy.

Until Active Directory prevails over the existing domain infrastructures, administrators and users are forced to use the Local Security Policy editor of individual Member Servers and Workstations 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.

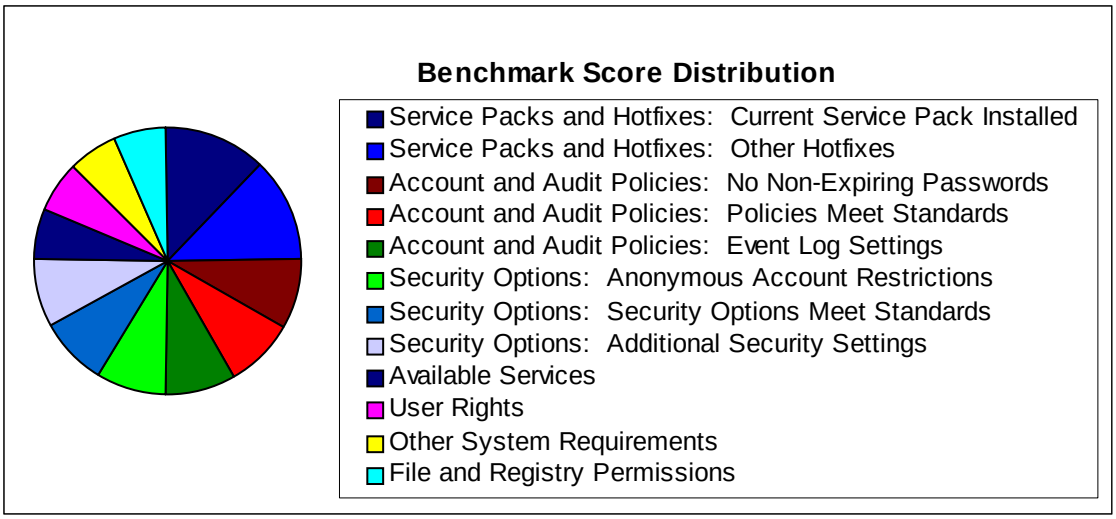
The actions required to "harden" a Windows 2000 operating system will be described in terms of updating the Local Security Policy. The Local Security Policy Editor, as well as many other tools used herein, is located in the Administrative Tools menu. In some cases, clicking the Start button, and then 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. **(A method involving the use of the Microsoft Security Configuration and Analysis Utility to automatically install the Win2kProGold_R1.2.inf template, which includes the security settings contained in this benchmark, is described in documentation that accompanies the CIS W2K scoring tool.**

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 four categories: (1) Service Packs and Hotfixes, (2) Policies, (3) Security Settings, and (4) Available Services, User Rights, File and Registry permissions, and Other System Requirements. Each category accounts for one quarter of the score. 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. Level II Benchmarks are being developed to cover such applications.

Each of the first three categories has a limited number of *major requirements* and many *minor requirements*. For example, in the area of Service Packs and Hotfixes, the current Service Pack is a major requirement, while other Hotfixes may be considered minor. The major and minor elements of each category are discussed in the following sections. The sections on Available Services and Other System Requirements have been added as a result of CIS member feedback.



As time goes on, these allocations are subject to change. This initial distribution pattern is only a starting point, and will undoubtedly be enhanced over time.

Section 1 – Summary Checklist

1 Service Packs and Hotfixes

1.1 Major Service Pack and Hotfix Requirements

1.1.1 Current Service Pack installed – **Service Pack 4 as of this writing.**

1.2 Minor Service Pack and Hotfix Requirements

1.2.1 All **Critical and Security Hotfixes** recognized by HFNetChk to date have been installed.

2 Auditing and Account Policies

2.1 Major Auditing and Account Policies Requirements

2.1.1 All passwords are **at least 8 characters long** (minimum).
2.1.2 All passwords are **no more than 90 days old** (maximum).

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: **Failure (minimum)**
2.2.1.6 Audit Policy Change: **Failure (minimum)**
2.2.1.7 Audit Privilege Use: **Failure (minimum)**
2.2.1.8 Audit Process Tracking: **Not Defined**
2.2.1.9 Audit System Events: **Success and Failure**

2.2.2 Account Policy

2.2.2.1 Minimum Password Age: **1 day**
2.2.2.2 Maximum Password Age: **90 days** (as per major requirements)
2.2.2.3 Minimum Password Length: **8 characters** (as per major requirements)
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**

2.2.3 Account Lockout Policy
2.2.3.1 Account Lockout Duration: **15 Minutes** (minimum)
2.2.3.2 Account Lockout Threshold: **3 Bad Login Attempts** (maximum)
2.2.3.3 Reset Account Lockout After: **15 Minutes** (minimum)

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: **80 Mb** (minimum)
2.2.4.1.2 Restrict Guest Access to Logs: **Enabled**
2.2.4.1.3 Log Retention Method: **"Overwrite Events As Needed"**
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** (minimum)
2.2.4.2.2 Restrict Guest Access to Logs: **Enabled**
2.2.4.2.3 Log Retention Method: **"Overwrite Events As Needed"**
2.2.4.2.4 Log Retention: **Not Defined**

2.2.4.3 System Log
2.2.4.3.1 Maximum Event Log Size: **80 Mb** (minimum)
2.2.4.3.2 Restrict Guest Access to Logs: **Enabled**
2.2.4.3.3 Log Retention Method: **"Overwrite Events As Needed"**
2.2.4.3.4 Log Retention: **Not Defined**

3 Security Settings

3.1 Major Security Settings
3.1.1 Additional Restrictions for Anonymous Connections: **"No Access Without Explicit Anonymous Permissions"**

3.2 Minor Security Settings

3.2.1 Security Options
3.2.1.1 Allow Server Operators to Schedule Tasks: **Not Applicable**
3.2.1.2 Allow System to be Shut Down Without Having to Log On: **Disabled**
3.2.1.3 Allowed to Eject Removable NTFS Media: **Administrators**
3.2.1.4 Amount of Idle Time Required Before Disconnecting Session: **30 Minutes** (minimum)
3.2.1.5 Audit the access of global system objects: **Not Defined**
3.2.1.6 Audit the use of backup and restore privilege: **Not Defined**
3.2.1.7 Automatically Log Off Users When Logon Time Expires: **Not Defined**

3.2.1.8 Automatically Log Off Users When Logon Time Expires (local): **Enabled**
3.2.1.9 Clear Virtual Memory Pagefile When System Shuts Down: **Enabled**
3.2.1.10 Digitally Sign Client Communication (Always): **Not Defined**
3.2.1.11 Digitally Sign Client Communication (When Possible): **Enabled**
3.2.1.12 Digitally Sign Server Communication (Always): **Not Defined**
3.2.1.13 Digitally Sign Server Communication (When Possible): **Enabled**
3.2.1.14 Disable CTRL+ALT+Delete Requirement for Logon: **Disabled**
3.2.1.15 Do Not Display Last User Name in Logon Screen: **Enabled**
3.2.1.16 LAN Manager Authentication Level: **"Send NTLMv2 response only"** (minimum)
3.2.1.17 Message Text for Users Attempting to Log On: **Custom Message** or "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."
3.2.1.18 Message Title for Users Attempting to Log On: "Warning:" or **custom title**.
3.2.1.19 Number of Previous Logons to Cache: **1** (maximum)
3.2.1.20 Prevent System Maintenance of Computer Account Password: **Disabled**
3.2.1.21 Prevent Users from Installing Printer Drivers: **Enabled**
3.2.1.22 Prompt User to Change Password Before Expiration: **14 Days** (minimum)
3.2.1.23 Recovery Console: Allow Automatic Administrative Logon: **Disabled**
3.2.1.24 Recovery Console: Allow Floppy Copy and Access to All Drives and All Folders: **Disabled**
3.2.1.25 Rename Administrator Account: **Any value other than 'Administrator'**
3.2.1.26 Rename Guest Account: **Any value other than 'Guest'**
3.2.1.27 Restrict CD-ROM Access to Locally Logged-On User Only: **Enabled**
3.2.1.28 Restrict Floppy Access to Locally Logged-On User Only: **Enabled**
3.2.1.29 Secure Channel: Digitally Encrypt or Sign Secure Channel Data (Always): **Not Defined**
3.2.1.30 Secure Channel: Digitally Encrypt Secure Channel Data (When Possible): **Enabled**
3.2.1.31 Secure Channel: Digitally Sign Secure Channel Data (When Possible): **Enabled**
3.2.1.32 Secure Channel: Require Strong (Windows 2000 or later) Session Key: **Not Defined**

An important question to ask: Is this computer a member of a Windows NT 4.0 Domain?

Yes: Enabling this setting requires that the domain infrastructure support 128 bit encryption. Do not enable this setting.
No: Windows 2000 or later domains are capable of supporting strong session keys. Enable this option.

3.2.1.33 Send Unencrypted Password to Connect to Third-Party SMB Servers: **Disabled**
3.2.1.34 Shut Down system immediately if unable to log security audits: **Not Defined**

3.2.1.35 Smart Card Removal Behavior: **"Lock Workstation"** (minimum)
3.2.1.36 Strengthen Default Permissions of Global System Objects (e.g. Symbolic Links): **Enabled**
3.2.1.37 Unsigned Driver Installation Behavior: **"Warn, but allow installation"** (minimum) or **"Do Not Allow Installation"**.
3.2.1.38 Unsigned Non-Driver Installation Behavior: **"Warn, but allow installation"** (minimum) or **"Do Not Allow Installation"**.

3.2.2 Additional Registry Settings
3.2.2.1 Suppress Dr. Watson Crash Dumps: **HKLM\Software\Microsoft\DrWatson\CreateCrashDump (REG_DWORD) 0**
3.2.2.2 Disable Automatic Execution of the System Debugger: **HKLM\ Software\Microsoft\Windows NT\CurrentVersion\ AEDebug\Auto (REG_DWORD) 0**
3.2.2.3 Disable autoplay from any disk type, regardless of application: **HKLM\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer\NoDriveTypeAutoRun (REG_DWORD) 255**
3.2.2.3.1 Disable autoplay for current user: **HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\ NoDriveTypeAutoRun (REG_DWORD) 255**
3.2.2.3.2 Disable autoplay for new users by default: **HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer\NoDriveTypeAutoRun (REG_DWORD) Not Defined**
3.2.2.4 Disable Automatic Logon: **HKLM\ Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon (REG_SZ) 0**
3.2.2.5 Don't display username of last successful logon at the logon screen: **HKLM\Software\Microsoft\Windows NT\ CurrentVersion\Winlogon\DontDisplayLastUserName (REG_SZ) Not Defined**
3.2.2.6 Enable the File System Checker and Disable Popups: **HKLM\ Software\Microsoft\Windows NT\CurrentVersion\ Winlogon\SFCDisable (REG_DWORD)** ***Not Defined***
3.2.2.7 Enable the System File Checker to verify all operating system files at boot time: **HKLM\Software\Microsoft\ Windows NT\CurrentVersion\Winlogon\SFCScan (REG_DWORD)** ***Not Defined***
Note: Due to the processor-intensive nature of the System File Checker, it is no longer required on startup.
3.2.2.8 Do not show the System File Checker progress meter: **HKLM\Software\Microsoft\Windows NT\CurrentVersion\ Winlogon\SFCShowProgress (REG_DWORD)** ***Not Defined***
3.2.2.9 Disable automatic reboots after a Blue Screen of Death: **HKLM\System\CurrentControlSet\Control\ CrashControl\AutoReboot (REG_DWORD) 0**
3.2.2.10 Disable CD Autorun: **HKLM\System\CurrentControlSet\Services\CDrom\Autorun (REG_DWORD) 0**
3.2.2.11 Remove administrative shares on workstation (Professional): **HKLM\System\CurrentControlSet\Services\ LanmanServer\Parameters\AutoShareWks (REG_DWORD) 0**

An important question to ask: Does this computer use administrative shares for remote backups, antivirus, or other remote administration activities?

Yes: Enabling this setting break remote administrative functionality. Be very careful implementing this setting. If you are unable to enable this setting because of the things it will break, please ask you software vendor to design future versions of the software to avoid this requirement. Do not enable this setting.

No: You will not be able to remotely administer the filesystems of this computer. Enable this option.

3.2.2.12 Protect against Computer Browser Spoofing Attacks: **HKLM\System\CurrentControlSet\Services\MrxSmb\Parameters\RefuseReset (REG_DWORD) 1**

3.2.2.13 Protect against source-routing spoofing: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting (REG_DWORD) 2**

3.2.2.14 Protect the Default Gateway network setting: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect (REG_DWORD) 0**

3.2.2.15 Ensure ICMP Routing via shortest path first: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect (REG_DWORD) 0**

3.2.2.16 Help protect against packet fragmentation: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery (REG_DWORD) 0**

3.2.2.17 Manage Keep-alive times: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime (REG_DWORD) 300000**

3.2.2.18 Protect Against Malicious Name-Release Attacks: **HKLM\System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand (REG_DWORD) 1**

3.2.2.19 Ensure Router Discovery is Disabled: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery (REG_DWORD) 0**

3.2.2.20 Protect against SYN Flood attacks: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect (REG_DWORD) 2**

3.2.2.21 SYN Attack protection – Manage TCP Maximum half-open sockets: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen (REG_DWORD) 100**

3.2.2.22 SYN Attack protection – Manage TCP Maximum half-open retired sockets: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetired (REG_DWORD) 80**

3.2.2.23 Enable IPSec to protect Kerberos RSVP Traffic: **HKLM\System\CurrentControlSet\Services\IPSEC\NoDefaultExempt (REG_DWORD) 1**

3.2.2.24 **HKLM\System\CurrentControlSet\Services\Lanmanserver\Parameters\Hidden (REG_DWORD) 1**

4 Additional Security Protection

4.1 Available Services

Permissions on services listed here: **Administrators: Full Control; System: Read, Start, Stop, and Pause**

4.1.1 Alerter – **Disabled**

4.1.2 Clipbook – **Disabled**

4.1.3 Computer Browser – **Disabled**

4.1.4 Fax Service – **Disabled**

4.1.5 FTP Publishing Service – **Disabled**

4.1.6 IIS Admin Service – **Disabled**
4.1.7 Internet Connection Sharing – **Disabled**
4.1.8 Messenger – **Disabled**
4.1.9 NetMeeting Remote Desktop Sharing – **Disabled**
4.1.10 Remote Registry Service – **Disabled**
4.1.11 Routing and Remote Access – **Disabled**
4.1.12 Simple Mail Transfer Protocol (SMTP) – **Disabled**
4.1.13 Simple Network Management Protocol (SNMP) Service – **Disabled**
4.1.14 Simple Network Management Protocol (SNMP) Trap – **Disabled**
4.1.15 Telnet – **Disabled**
4.1.16 World Wide Web Publishing Services – **Disabled**
4.1.17 Automatic Updates – **Not Defined**
4.1.18 Background Intelligent Transfer Service – **Not Defined**

4.2 User Rights
4.2.1 Access this computer from the network: **Users, Administrators (or none)**
4.2.2 Act as part of the operating system: **None**
4.2.3 Add workstations to domain: **Not applicable**
4.2.4 Back up files and directories: **Administrators**
4.2.5 Bypass traverse checking: **Users**
4.2.6 Change the system time: **Administrators**
4.2.7 Create a pagefile: **Administrators**
4.2.8 Create a token object: **None**
4.2.9 Create permanent shared objects: **None**
4.2.10 Debug Programs: **None**
4.2.11 Deny access to this computer from the network: **Guests**
4.2.12 Deny logon as a batch job: **None by default (others allowable as appropriate)**
4.2.13 Deny logon as a service: **None by default (others allowable as appropriate)**
4.2.14 Deny logon locally: **None by default (others allowable as appropriate)**
4.2.15 Enable computer and user accounts to be trusted for delegation: **Not Applicable**
4.2.16 Force shutdown from a remote system: **Administrators**
4.2.17 Generate security audits: **None**
4.2.18 Increase quotas: **Administrators**
4.2.19 Increase scheduling priority: **Administrators**
4.2.20 Load and unload device drivers: **Administrators**
4.2.21 Lock pages in memory: **None**

4.2.22 Log on as a batch job: **None**
4.2.23 Log on as a service: **None**
4.2.24 Log on locally: **Users, Administrators (further restriction allowable)**
4.2.25 Manage auditing and security log: **Administrators**
4.2.26 Modify firmware environment values: **Administrators**
4.2.27 Profile single process: **Administrators**
4.2.28 Profile system performance: **Administrators**
4.2.29 Remove computer from docking station: **Users, Administrators**
4.2.30 Replace a process level token: **None**
4.2.31 Restore files and directories: **Administrators**
4.2.32 Shut down the system: **Users, Administrators**
4.2.33 Synchronize directory service data: **Not Applicable**
4.2.34 Take ownership of file or other objects: **Administrators**

4.3 Other System Requirements

4.3.1 Ensure all disk volumes are using the **NTFS file system**

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. Creator Owner Full Control is for subfolders and files only. Users permissions are for current folder, subfolders, and files.

4.4.1.1 %SystemDrive%\ - **Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List**
4.4.1.2 %SystemDrive%\autoexec.bat – **Administrators: Full; System: Full**
4.4.1.3 %SystemDrive%\boot.ini – **Administrators: Full; System: Full**
4.4.1.4 %SystemDrive%\config.sys - **Administrators: Full; System: Full**
4.4.1.5 %SystemDrive%\io.sys – **Administrators: Full; System: Full**
4.4.1.6 %SystemDrive%\msdos.sys – **Administrators: Full; System: Full**
4.4.1.7 %SystemDrive%\ntbootdd.sys - **Administrators: Full; System: Full**
4.4.1.8 %SystemDrive%\ntdetect.com – **Administrators: Full; System: Full**
4.4.1.9 %SystemDrive%\ntldr - **Administrators: Full; System: Full**
4.4.1.10 %SystemDrive%\Documents and Settings – **Administrators: Full; System: Full; Users: Read and Execute, List**
4.4.1.11 %SystemDrive%\Documents and Settings\Administrator – **Administrators: Full; System: Full**
4.4.1.12 %SystemDrive%\Documents and Settings\All Users – **Administrators: Full; System: Full; Users: Read and Execute, List**
4.4.1.13 %SystemDrive%\Documents and Settings\All Users\Documents \DrWatson – **Administrators: Full; System: Full; Creator Owner: Full; Users: Traverse Folder/Execute File, List Folder/Read Data, Read Attributes, Read Extended**

Attributes, Read Permissions (This folder, subfolders, and files); Users: Traverse Folder/Execute Files, Create Files/Write Data, Create Folder/Append Data (Subfolders and files only)

4.4.1.14 %SystemDrive%\Documents and Settings\Default User – **Administrators: Full; System: Full; Users: Read and Execute, List**

4.4.1.15 %ProgramFiles% - **Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List**

4.4.1.16 %Program Files%\Resource Kit – **Administrators: Full; System: Full**

4.4.1.17 %Program Files%\Resource Pro Kit – **Administrators: Full; System: Full**

4.4.1.18 %SystemRoot% – **Administrators: Full; System: Full; Creator Onwer: Full; Users: Read and Execute, List**

4.4.1.19 %SystemRoot%\$NtServicePackUninstall$ – **Administrators: Full; System: Full**

4.4.1.20 %SystemRoot%\CSC – **Administrators: Full; System: Full**

4.4.1.21 %SystemRoot%\Debug - **Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List**

4.4.1.22 %SystemRoot%\Debug\UserMode - **Administrators: Full; System: Full; Users: Traverse Folder/Execute File, List folder/Read data, Create files/Write data (This folder, only); Create files/Write data, Create folders/Append data (Files only)**

4.4.1.23 %SystemRoot%\Offline Web Pages – **Ignore Parent Permission Changes**

4.4.1.24 %SystemRoot%\Registration - **Administrators: Full; System: Full; Users: Read**

4.4.1.25 %SystemRoot%\repair - **Administrators: Full; System: Full**

4.4.1.26 %SystemRoot%\security - **Administrators: Full; System: Full; Creator Owner: Full**

4.4.1.27 %SystemRoot%\system32 - **Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List**

4.4.1.28 %SystemRoot%\system32\at.exe – **Administrators: Full; System: Full**

4.4.1.29 %SystemRoot%\system32\Ntbackup.exe – **Administrators: Full; System: Full**

4.4.1.30 %SystemRoot%\system32\rcp.exe – **Administrators: Full; System: Full**

4.4.1.31 %SystemRoot%\regedit.exe – **Administrators: Full; System: Full**

4.4.1.32 %SystemRoot%\system32\regedt32.exe – **Administrators: Full; System: Full**

4.4.1.33 %SystemRoot%\system32\rexec.exe – **Administrators: Full; System: Full**

4.4.1.34 %SystemRoot%\system32\rsh.exe – **Administrators: Full; System: Full**

4.4.1.35 %SystemRoot%\system32\secedit.exe – **Administrators: Full; System: Full**

4.4.1.36 %SystemRoot%\system32\appmgmt – **Administrators: Full; System: Full; Users: Read and Execute, List**

4.4.1.37 %SystemRoot%\system32\config – **Administrators: Full; System: Full**

4.4.1.38 %SystemRoot%\system32\dllcache – **Administrators: Full; System: Full; Creator Owner: Full**

4.4.1.39 %SystemRoot%\system32\DTCLog - **Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List**

4.4.1.40 %SystemRoot%\system32\Group Policy - **Administrators: Full; System: Full; Authenticated Users: Read and Execute, List**

4.4.1.41 %SystemRoot%\system32\ias - **Administrators: Full; System: Full; Creator Owner: Full**

4.4.1.42 %SystemRoot%\system32\NTMSData – **Administrators: Full; System: Full**
4.4.1.43 %SystemRoot%\system32\reinstallbackups – **Administrators: Full; System: Full; Creator Owner: Full; Power Users: Read and Execute, List**
4.4.1.44 %SystemRoot%\system32\Setup – **Administrators: Full; System: Full; Users: Read and Execute, List**
4.4.1.45 %SystemRoot%\system32\spool\printers – **Administrators: Full; System: Full; Creator Owner: Full; Users: Traverse Folder, Execute File, Read, Read Extended Attributes, Create folders, Append Data**
4.4.1.46 %SystemRoot%\Tasks - **(Do not allow permissions on this folder to be replaced)**
4.4.1.47 %SystemDrive%\System Volume Information – **(Do not allow permissions on this folder to be replaced)**

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\Classes - **Administrators: Full; System: Full; Creator Owner: Full; Users: Read**
4.4.2.2 HKLM\Software – **Administrators Full; System: Full; Creator Owner: Full; Users: Read**
4.4.2.3 HKLM\Software\Microsoft\Net DDE – **Administrators: Full; System: Full**
4.4.2.4 HKLM\Software\Microsoft\OS/2 Subsystem for NT – **Administrators: Full; System: Full; Creator Owner: Full**
4.4.2.5 HKLM\Software\Microsoft\Windows NT\CurrentVersion\AsrCommands – **Administrators: Full; System: Full; Creator Owner: Full; Users: Read; Backup Operators: Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read (this key and subkeys)**
4.4.2.6 HKLM\Software\Microsoft\Windows NT\CurrentVersion\Perflib – **Administrators: Full; System: Full; Creator Owner: Full; Interactive: Read (this key and subkeys)**
4.4.2.7 HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy - **Administrators: Full; System: Full; Authenticated Users: Read**
4.4.2.8 HKLM\Software\Microsoft\Windows\CurrentVersion\Installer - **Administrators Full; System: Full; Users: Read**
4.4.2.9 HKLM\Software\Microsoft\Windows\CurrentVersion\Policies - **Administrators: Full; System: Full; Authenticated Users: Read**
4.4.2.10 HKLM\System - **Administrators Full; System: Full; Creator Owner: Full; Users: Read**
4.4.2.11 HKLM\System\Clone – **Allow inheritable permissions to propagate to this object**
4.4.2.12 HKLM\System\ControlSet001 - **Administrators Full; System: Full; Creator Owner: Full; Users: Read**
4.4.2.13 HKLM\System\ControlSet00x - **Administrators Full; System: Full; Creator Owner: Full; Users: Read**

* Apply these permissions to all control sets other than CurrentControlSet.

4.4.2.14 HKLM\System\CurrentControlSet\Control\SecurePipeServers\WinReg – **Administrators: Full**
4.4.2.15 HKLM\System\CurrentControlSet\Control\WMI\Security – **Administrators: Full; System: Full; Creator Owner: Full (this key and subkeys)**
4.4.2.16 HKLM\System\CurrentControlSet\Enum - **(Do not allow permissions on this key to be replaced)**

4.4.2.17 HKLM\System\CurrentControlSet\Hardware Profiles – **Administrators Full; System: Full; Creator Owner: Full; Users: Read**
4.4.2.18 HKLM\System\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers - **Administrators Full; System: Full; Creator Owner: Full**
4.4.2.19 HKLM\System\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities - **Administrators Full; System: Full; Creator Owner: Full**
4.4.2.20 HKU\.Default - **Administrators Full; System: Full; Creator Owner: Full; Users: Read**
4.4.2.21 HKU\.Default\Software\Microsoft\NetDDE - **Administrators Full; System: Full**
4.4.2.22 HKU\.Default\Software\Microsoft\Protected Storage System Provider – **No entries**

4.4.3 File and Registry Auditing
4.4.3.1 %SystemDrive% - **Everyone: Failures (this folder, propagate inheritable permissions to all subfolders and files)**
4.4.3.2 HKLM\Software – **Everyone: Failures (this key, propagate inheritable permission to all subkeys)**
4.4.3.3 HKLM\System – **Everyone: Failures (this key, propagate inheritable permission to all subkeys)**

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 2000 system that is completely current on Windows 2000 Hotfixes and Service Packs also needs to be kept current with Service Packs and Hotfixes for Internet Explorer and MS 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

At the time of this writing, Windows 2000 Service Pack 4 is available.

WARNING: Although Service Packs are generally reliable and go through extensive testing, it is possible 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.

1.2 Minor Service Pack and Hotfix Requirements

1.2.1 All Critical Hotfixes available to date have been installed.

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.

2 Auditing and Account Policies

2.1 Major Auditing and Account Policies Requirements

2.1.1 All passwords are **at least 8 characters long** (minimum).

There is an ongoing debate as to whether complex passwords that are longer than 7 characters are any more secure than passwords of exactly 7 characters, or passwords that are multiples of 7 characters. The overriding factor is that password complexity within each block of 7 characters determines how difficult passwords are to crack, with regards to LAN Manager password hashes. The general consensus is that passwords of 8 or more characters, when combined with other factors discussed herein, make passwords very difficult to crack.

2.1.2 All passwords are **no more than 90 days old** (maximum).

Many systems and network administrators and help desk personnel spend significant time and effort ensuring that users change their passwords on a regular basis. This is a part of system administration that affects every user in a domain. What many people overlook is that each Windows 2000 Professional computer has at least one "Administrator" account and one "Guest" account. The guest account is disabled by default, but the Administrator never disables, never locks out, and has full reign over that workstation. These passwords are often left unchanged for the life of a computer.

In addition, there may be service accounts with elevated privileges that never have their password changed either. Administrator or privileged accounts with passwords that never change are prime targets for an intruder, and make it easy to gain an initial foothold into a computer, company workgroup, or domain.

2.2 Minor Auditing and Account Policies Requirements

2.2.1 Audit Policy (minimums)

The "Audit Policy" determines what sort of system events the computer tracks or records for administrators to determine what has actually happened over time. The events may be used to track events that an application performed, or events that a user performed. They may also indicate attempts by unauthorized network users to penetrate a computer from the user console or the network. There are a number of security related events that should be recorded, but none are recorded by default.

Click the Start button and navigate to Settings, and the Control Panel. Double-click "Administrative Tools". Then double-click "Local Security Policy". In the left pane, expand Local Policies, and click Audit Policy. To make changes, double-click one of the settings in the right pane, check or uncheck the appropriate boxes, and click OK to save the settings. They will take effect when the Local Security Policy editor is closed.

2.2.1.1 Audit Account Logon Events: **Success and Failure**

Auditing logon events will track successful and failed logon attempts from the local console, the network, or batch or service accounts using domain logon credentials. If a user attempts to log on and fails, the only way to know will be to have this auditing enabled, and to periodically check the local machine's Security Event Log.

2.2.1.2 Audit Account Management: **Success and Failure**

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.

2.2.1.3 Audit Directory Service Access: **Not Defined**

No auditing of Directory Service Access is required on Windows 2000 Professional because Directory Service Access can only be audited on Windows 2000 (or later) domain controllers.

2.2.1.4 Audit Logon Events: **Success and Failure**

Auditing logon events will track successful and failed logon attempts from the local console, the network, or batch or service accounts using local machine logon credentials. If a user attempts to log on and fails, the only way to know will be to have this auditing enabled, and to periodically check the local machine's Security Event Log.

2.2.1.5 Audit Object Access: **Failure (minimum)**

It is possible to track when specific users access specific files. In order to track users access to files, go to that file or folder, edit the security properties for that object, and enable auditing for specific users on those objects.

Also, enable Audit Object Access for success or failure here, and each audit that fulfills your requirements will produce an event in the security event log. Enabling this option in the audit policy does not produce events itself, unless objects and users are actively being audited.

2.2.1.6 Audit Policy Change: **Failure (minimum)**

If audit policies are audited, changes to User Rights, Audit Policies, or Trust Policies will produce events in the Security Event Log.

2.2.1.7 Audit Privilege Use: **Failure (minimum)**

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 if a user or process attempts to bypass traverse checking, debug programs, create a token object, replace a process level token, or generate security audits. It will also generate events if a user or account attempts to backup or restore files or directories using the Backup or Restore user right, but only if the security option to audit backups and restores is enabled.

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. This is normal, and sorting through these events is part of the cost of detailed auditing.

2.2.1.8 Audit Process Tracking: **Optional**

Each time an application or a user starts, stops, or otherwise changes a process, it will create an event in the event log. 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. As such, auditing process tracking is not required, and is only recommended when absolutely necessary.

2.2.1.9 Audit System Events: **Success and Failure**

Auditing System events is very important. System events include starting or shutting down the computer, full event logs, or other security related events that have impact across the entire system. Auditing of Success and Failure events should be enabled.

2.2.2 Account Policy

2.2.2.1 Minimum Password Age: **1 day**

If users are required to change their passwords, and the operating system remembers a certain number of passwords, the only way to keep users from cycling through the number of passwords is to set a minimum life time requirement for each new password once it was changed. As long as this is set to a time greater than zero, users are unable to cycle back to their favorite password.

2.2.2.2 Maximum Password Age: **90 days** (as per major requirements)

Many systems and network administrators and help desk personnel spend significant time and effort ensuring that users change their passwords on a regular basis. This is a part of system administration that affects every user in a domain. What many people overlook is that each Windows 2000 Professional computer has at least one "Administrator" account and one "Guest" account. The guest account is disabled by default, but the Administrator never disables, never locks out, and has full reign over that workstation. These passwords are often left unchanged for the life of a computer.

In addition, there may be service accounts with elevated privileges that never have their password changed either. Administrator or privileged accounts with passwords that never change are prime targets for an intruder, and make it easy to gain an initial foothold into a computer, company workgroup, or domain.

2.2.2.3 Minimum Password Length: **8 characters** (as per major requirements)

There is an ongoing debate as to whether complex passwords that are longer than 7 characters are any more secure than passwords of exactly 7 characters, or passwords that are multiples of 7 characters. The overriding factor is that password complexity within each block of 7 characters determines how difficult passwords are to crack, with regards to LAN Manager password hashes. The general consensus is that passwords of 8 or more characters, when combined with other factors discussed herein, make passwords very difficult to crack.

2.2.2.4 Password Complexity: **Enabled**

Passwords are made up of various characters, which can be broken down into four character groups. These are uppercase alphabetic, lowercase alphabetic, numeric, and special characters. Requiring complex passwords will require new passwords to use characters from three of those four groups.

Complex passwords become difficult for users to remember, easier to mistype, and result in more users calling support personnel for password assistance. Requiring complex passwords also increases the time necessary to crack passwords exponentially.

2.2.2.5 Password History: **24 Passwords Remembered**

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.

2.2.2.6 Store Passwords using Reversible Encryption: **Disabled**

One of the rare strengths of the Windows password models is that they use one-way encryption. That is, the passwords are encrypted to a numeric value, called a "hash". This hash can not be decrypted to directly discover the original password.

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.

2.2.3 Account Lockout Policy

One of the older methods used to guess a user's password was to repeatedly attempt to access a computer using a logical or known account name, and a constantly changing password until one succeeds. In order to counter the usefulness of this attack, account authorizations can be set to "lock out" an account if too many login attempts (Account Lockout Threshold) are made in a determined period of time (Reset Account Lockout) for a period of time(Lockout Duration). If an account is locked out, it refuses to authenticate that account, until the locked out account is reset – either automatically, or by an administrator.

2.2.3.1 Account Lockout Duration: **15 Minutes** (minimum)
2.2.3.2 Account Lockout Threshold: **3 Bad Login Attempts** (maximum)
2.2.3.3 Reset Account Lockout After: **15 Minutes** (minimum)

2.2.4 Event Log Settings – Application, Security, and System Logs

When events are audited, they are stored in one of the Windows Event Logs. The three event logs common to all Windows computers are the Application, Security, and System logs. Obviously, the Security event log potentially holds most of the relevant details for a security standard, but in the event that administrators need to reconstruct events that have occurred, any source of information can be significant, so all logs need to be addressed.

The default size of each event log is 512k. This has been standard since the days of Windows NT 3.5, when a 2 GB hard drive was a rare thing, and a 40 GB hard drive was only a dream. Using modern hardware, 80 MB of hard drive space for each event log should not be a burden. Access to event logs should be restricted from guest access. Log retention should normally set to overwrite events "as needed" unless an administrator is earnestly going to be checking the logs on a regular basis, in which case it should be set to retain logs "by days" and the Log Retention should be set to at least 14 days, or as long as it takes for an administrator to archive the event logs on another system.

2.2.4.1 Application Log
2.2.4.1.1 Maximum Event Log Size: **80 Mb** (minimum)
2.2.4.1.2 Restrict Guest Access to Logs: **Enabled**
2.2.4.1.3 Log Retention Method: **"Overwrite Events As Needed"**
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** (minimum)
2.2.4.2.2 Restrict Guest Access to Logs: **Enabled**
2.2.4.2.3 Log Retention Method: **"Overwrite Events As Needed"**
2.2.4.2.4 Log Retention: **Not Defined**

2.2.4.3 System Log

2.2.4.3.1 Maximum Event Log Size: **80 Mb** (minimum)
2.2.4.3.2 Restrict Guest Access to Logs: **Enabled**
2.2.4.3.3 Log Retention Method: **"Overwrite Events As Needed"**
2.2.4.3.4 Log Retention: **Not Defined**

3 Security Settings

Security settings are changed in the Local Security Policy Editor. Expand Local Policies to Security Options. Double-click a setting, make the appropriate changes, and click OK. Once the Local Security Policy Editor is closed, the settings will take effect.

3.1 Major Security Settings

Click the Start button and navigate to Settings, and the Control Panel. Double-click "Administrative Tools". Then double-click "Local Security Policy". In the left pane, 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. They will become effective immediately, but won't show up in the Local Security Policy editor until it is closed.

3.1.1 Additional Restrictions for Anonymous Connections: **"No Access Without Explicit Anonymous Permissions"**

The first setting under "Security Options" is "Additional Restrictions for Anonymous Connections". It can be set to "None. Rely on default permissions", "Do not allow enumeration of SAM accounts or shares", or "No access without explicit anonymous permissions". Change this setting to the last choice, and protect your computer from access by the Null User account.

WARNING: Note that doing so may disable older programs that make use of this account. It will also hamper Windows NT 4.0 Domain Controllers from communicating with each other between trust relationships. Personal users probably don't have to worry about this setting, but should be wary if something doesn't work right after it is changed. Corporate or Government users should test this in an extensive lab environment before mandating it among many users.

3.2 Minor Security Settings

3.2.1 Security Options

3.2.1.1 Allow Server Operators to Schedule Tasks: **Not Applicable**

This setting is designed for Windows 2000 Server Domain Controllers. It has no effect on Windows 2000 Professional computers.

3.2.1.2 Allow System to be Shut Down Without Having to Log On: **Disabled**

By default, Windows 2000 Professional enables this option, and Windows 2000 Servers disable it. While logging on to shut down a system may be an inconvenience, it is necessary to ensure that the workstation is not rebooted without the users' knowledge.

3.2.1.3 Allowed to Eject Removable NTFS Media: **Administrators**

Which users are permitted to remove NTFS formatted media from computers. This generally applies to removable disks, JAZ or ZIP drives. If other users need to be granted this right, add them to the list, but the only group that should be listed here is Administrators.

3.2.1.4 Amount of Idle Time Required Before Disconnecting Session: **30 Minutes** (maximum)

When Windows computers begin a connection with each other, they exchange username and password credentials, authenticating and authorizing use of shared resources. After a certain period of inactivity, that connection needs to be re-authenticated to ensure that the network connection is still originating from the correct valid user. The default value of 15 minutes is sufficient for most networks. Computers that do not share resources with other Windows computers are not affected by this setting.

3.2.1.5 Audit the access of global system objects: **Not Defined**

One of the types of auditing that Windows is capable of is the auditing of Global System Objects. These kernel objects, such as mutexes, semaphores, and DOS devices are normally audited by developers because they indicate programmatic behavior within the kernel. Normal system operation does not need to be audited in such detail. This setting is optional.

3.2.1.6 Audit the use of backup and restore privilege: **Not Defined**

Another thing that Windows can audit is the use of the Backup Files or Restore Files privilege. When enabled, this will cause an event to be generated every time a file is backed up or restored. You can imagine that this will generate a significant number of events for normal operation. This setting is also optional.

3.2.1.7 Automatically Log Off Users When Logon Time Expires: **Not Defined**

Not configurable on a local Windows 2000 Machine – This is a domain setting only.

3.2.1.8 Automatically Log Off Users When Logon Time Expires (local): **Enabled**

This setting is identical to the previous setting except that it applies to local accounts, where 3.2.1.7 applies to domain accounts, and is normally applied through Group Policy.

3.2.1.9 Clear Virtual Memory Pagefile When System Shuts Down: **Enabled**

As part of the normal behavior of a computer, not all of the “memory” being used is kept in the physical memory of a computer. Some of that memory is temporarily swapped or “paged” to disk when it is not in use. This benefits by allowing the computer to act like it has significantly more memory than it actually has. This was a lot more important when 128 MB of memory was prohibitively expensive, if you could manage to find it.

The memory saved to disk is not supposed to contain cryptographic keys or logon credentials, but the usernames and passwords that are not integrated into the operating system are subject to being stored in the page file. When a computer is shut down, that pagefile is not normally overwritten. Anyone who can boot the computer to an alternate operating system can examine that disk space, and obtain any sort of sensitive information that was written to the pagefile.

Enable this option to clear the pagefile on shutdown. This will ensure that any sensitive information is overwritten as the machine shuts down. Be aware that this will also increase

the time that a computer takes to shut down, and also start up. How long depends on how fast the computer is, and how big the pagefile is.

3.2.1.10 Digitally Sign Client Communication (Always): **Not Defined**

When one computer initiates a remote procedure call (RPC) with another, the computer that starts the conversation is the "client" and the computer fulfilling the request is the "server" regardless of whether or not the computer is a workstation or server. If you require this option, any time this computer acts as a "client" the server must also support digital signatures, or the requesting client will not permit the connection to complete.

Digitally signing such communication is always a good idea, however if you require it all of the time, any situation that prevents it will prevent the session entirely. If you have a network that you can guarantee that all computers are capable of signing client communication, by all means, please do so. In most cases, the next option is more realistic.

3.2.1.11 Digitally Sign Client Communication (When Possible): **Enabled**

When possible, digitally sign client communication. If not possible, for whatever reason, client communication will not be signed, but communication will be permitted. This is the best option for widespread acceptance. This is enabled by default.

3.2.1.12 Digitally Sign Server Communication (Always): **Not Defined**

Just like 3.2.1.10, any time this computer acts as a server, or is answering requests from another computer, that computer must allow for signing ITS client session, or no session can be established. This may be desirable, but be careful when implementing it. It is not required.

3.2.1.13 Digitally Sign Server Communication (When Possible): **Enabled**

It is still a good idea to digitally sign server communication from your local computer, and enabling this option to sign it "when possible" is a harmless way to ensure that traffic is signed when possible. This option is enabled by default, and should remain enabled.

3.2.1.14 Disable CTRL+ALT+Delete Requirement for Logon: **Disabled**

The CTRL+ALT+Delete requirement for logon, by itself, is a very strong aid to the security of a Windows computer. There are tools available that can circumvent many aspects of Windows security, but the CTRL+ALT+Delete at least makes it difficult to subvert the operating system.

That being said, this is one of the most confusing settings that Microsoft has ever given to the rest of the world. Look back at the name of the setting: "Disable CTRL+ALT+Delete…" This setting must be disabled to REQUIRE the CTRL+ALT+Delete for logon. Once again, that's DISABLE the "Disable CTRL+ALT+Delete Requirement for Logon" setting.

3.2.1.15 Do Not Display Last User Name in Logon Screen: **Enabled**

Anyone who walks up to a computer and presses CTRL+ALT+Delete can see the name of the last valid user who logged on to that system. As a result, they now have the name of a valid user for that computer. While it is true that there are other ways to garner that information, every little bit helps. Enable this setting to suppress the display of the last username.

WARNING: If you are enabling this setting in a multi-user environment, you can expect some users to call the help desk and complain because you taking something away that they

are accustomed to. The keys to making this sort of policy stick are to first get management approval and support, and second communicate your intentions ahead of time. Once the change is made, it should not be a shock to your users.

3.2.1.16 LAN Manager Authentication Level: **"Send NTLMv2 response only"** (minimum)

Windows network authentication has gone through some growing pains, and as a result has evolved quite a bit. The original LAN Manager (or LM) password hash is considered very weak. 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.

During the life of Windows NT 4.0, Microsoft developed the NTLM password hash and the NTLM version 2 (NTLMv2) password hash, which are significantly more difficult to break. All of these authentication methods are incorporated into Windows 2000.

The problem with password hashes is that 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. There are six choices available to determine what type of authentication is used and/or acceptable:

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 is the first and weakest – 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". Enable more strict security if you are able to require it across your entire network.

WARNING: 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 will require them to have installed the DSCLIENT.EXE utility from the Windows 2000 installation CD.

3.2.1.17 Message Text for Users Attempting to Log On: **Custom Message** or "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."

There is a legal precedence in this country that says an intruder in a network or computer system is not an intruder unless he has been warned that he is not welcome on that system, and he accepts the fact that, by entering that computer system, his acts may be monitored. This is the equivalent of a digital "No Trespassing" sign, commonly called a Banner.

The sample banner provided above is an approved banner provided by the United States Department of Justice. It has been deemed suitable by the government. If your organization expects to prosecute criminal behavior detected on their networks, you are advised to have this sample banner approved by your own legal counsel, or ask them to suggest and approve one for your organization.

3.2.1.18 Message Title for Users Attempting to Log On: "Warning:" or **custom title**.

The message title goes hand-in-hand with the message text. No matter what else you put in your message title and text, don't say "Welcome". Remember that you are warning potential intruders away. You don't want anything that can be construed as an invitation.

3.2.1.19 Number of Previous Logons to Cache: **1** (maximum)

"Cached logon credentials" has no effect unless the computer is a member of a domain, and the user logs on using a domain account. If a user logs on to a computer through a domain account, then takes that computer off the network, he or she will need to authenticate somewhere to gain controlled access to the computer. Windows retains or caches the logon credentials of some number of users (default is 10) so that if they logged in before, they will be able to log on again if the computer can't reach a domain controller to authenticate the user.

The preferred value for this setting is zero – to disallow any user from logging on to a computer if it is unable to contact a domain. Unfortunately, that will also render most corporate laptops entirely unusable. In order to accommodate those users, set this value to 1. That will allow ONLY the last user who successfully logged on to the computer to log on when it is disconnected from the network.

3.2.1.20 Prevent System Maintenance of Computer Account Password: **Disabled**

Most people are unaware that when a computer is part of a domain, that computer has its own account name and password (separate from usernames and their passwords) that authenticates against the domain. Since that happens, it is potentially possible to gain some access to a domain using the computer's account and password.

Windows 2000 computers are capable of periodically changing the password to their machine account on a regular basis, requiring no action on the part of the user – their username and password is entirely separate from that of the computer. Leave this option enabled to allow domain members to protect their accounts' passwords.

This has no effect unless the computer is a member of a domain.

3.2.1.21 Prevent Users from Installing Printer Drivers: **Enabled**

When printer drivers are installed onto an operating system, their code is installed directly into the privileged space of the operating system kernel. This allows printer drivers to accomplish tasks that are beyond the actual user's capability. Unfortunately, it also opens the operating system up to execute malicious code in the form of a "Trojan Horse" printer driver.

WARNING: Restricting the ability of users to install their own printer drivers will cause an increased number of support calls, both for the help desk and desktop visits. You should be aware of this, and plan accordingly.

3.2.1.22 Prompt User to Change Password Before Expiration: **14 Days** (minimum)

Part of the password cycle is to notify users when their password is in danger of expiring. Give users plenty of notice so that they can change their password in time to avoid more help desk calls. 14 days should exceed most other commitments, including most vacations.

3.2.1.23 Recovery Console: Allow Automatic Administrative Logon: **Disabled**

One of the features new to Windows 2000 is the Recovery Console. The Recovery Console gives limited command-line access to an otherwise unbootable operating system.

It was developed in response to the fact that the NTFS file system does not natively allow access if 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.

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. Bear in mind that this is not *any* administrator, but *the* Administrator. If the Administrator account has been renamed (as it should) you still need the password for that account.

Also built into the Recovery Console is this security setting, and the next one. This setting allows Administrators to remove the requirement for anyone who can reboot the computer, to bypass all security and directly access the operating system. This is generally accepted as a bad idea. Disable this setting, and keep positive track of the password to your local Administrator account.

3.2.1.24 Recovery Console: Allow Floppy Copy and Access to All Drives and All Folders: **Disabled**

One of the other features of the Windows 2000 Recovery Console is that it does not allow access to all files and folders on the hard drives. It allows access to the root folder of each volume, and the %systemroot% folder, normally c:\winnt and its subfolders. Even then, it does not allow the operator to copy files from the hard drive to removable media.

The "Recovery Console: Allow Floppy Copy and Access to All Drives and All Folders" Security Setting is designed to optionally circumvent the Recovery Console's ability to protect the operating system. This setting is disabled by default, and it should remain disabled.

3.2.1.25 Rename Administrator Account: **Any value other than 'Administrator'**

The only credentials required to access a computer, either at the console or on a network are a valid username, and its password. Windows creates a default privileged account named "Administrator".

Change this account name to something site-specific. The account still needs to be accessible for valid access, but needs to be less predictable than a default installation allows. Please note that this does not provide a great deal of protection against an experienced attacker, but it *may* protect against scripted attacks.

3.2.1.26 Rename Guest Account: **Any value other than 'Guest'**

Unlike the default Administrator account, the Guest account is disabled by default. It is only used to allow access to unauthenticated users, and then only if the account has a null

password and it is not disabled. The Guest account has more safeguards in place, and is not as much a target as the Administrator account, but it still deserves significant attention to maintain security.

Like the default Administrator account, the Guest account still needs to be protected. Change this to a site-specific name to help protect against its use.

3.2.1.27 Restrict CD-ROM Access to Locally Logged-On User Only: **Enabled**

It is possible for workstations to share files and folders from anywhere in their filesystem. As a result, the CD-ROM drive can be shared externally. Enabling this setting will prevent anyone but the currently logged on user from accessing material on the CD-ROM drive.

WARNING: One problem has been identified when this setting is enabled. When users are installing software from a CD-ROM drive, and those installation packages use the Microsoft Installer (.MSI) packages, the software is actually installed by the Windows Installer service, NOT the local 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.

3.2.1.28 Restrict Floppy Access to Locally Logged-On User Only: **Enabled**

Just like the CD-ROM drive, the floppy drive can be shared to allow network users access to the files on the floppy disk. This usually represents more of a risk than access to the CD-ROM because most CDs (but not all) are manufactured, and commercially available, while most of the data copied to a floppy drive is proprietary. Whether or not that is the case, enable this setting to prevent sharing of the floppy disk drive.

3.2.1.29 Secure Channel: Digitally Encrypt or Sign Secure Channel Data (Always): **Not Defined**

Secure Channels are normally established between workstations or servers and Domain Controllers. This data can include password authentication hashes. Signing the data encapsulates it in a digital signature that authenticates the recipient. Encrypting the data signs it and masks it, making the data indecipherable if it is intercepted over the network. If a computer is unable to connect to a Domain Controller by a signed or encrypted channel, no session will be established. Generally, this option should be disabled unless the computer is in a domain where all machines have this option enabled.

3.2.1.30 Secure Channel: Digitally Encrypt Secure Channel Data (When Possible): **Enabled**

As described above, “encrypting” the secure channel authenticates the computers at both ends of the conversation (signs) and encrypts the data to prevent interception of that data. This option should be enabled. It has no effect outside of a domain environment.

3.2.1.31 Secure Channel: Digitally Sign Secure Channel Data (When Possible): **Enabled**

Digitally signing the Secure Channel data provides authentication of all members of a “Conversation” and prevents a “Man in the middle” type of attack. This option should be enabled, but also has no effect outside of a domain environment.

3.2.1.32 Secure Channel: Require Strong (Windows 2000 or later) Session Key: **Not Defined**

When a Secure Channel is signed or encrypted, or when anything is signed or encrypted, one of the key factors is what strength of encryption is used. Windows 2000 Domains are capable of using 128-bit encryption. This is the default setting, and should be used when possible. Windows NT 4.0 domains are not capable of using this high encryption, and if this option is required, it may actually force the Secure Channel to be established without any signing or encryption because the domain is not capable of maintaining this high level of encryption.

As a standard, this setting should be enabled. In a Windows NT domain, disable the setting. In a Windows 2000 domain, enable this setting.

3.2.1.33 Send Unencrypted Password to Connect to Third-Party SMB Servers: **Disabled**

The end result of this setting can be determined answering one question: When your Windows 2000 computer requests authentication with a non-Windows computer, should your Windows computer send your password in cleartext to that computer? You don't have to think very hard about this setting to realize that it presents a serious risk to network security. This is disabled by default, and it should remain so.

If you find an application that requires this setting to be enabled, please first send feedback to windows-feedback@cisecurity.org so we can document it, and second, write to the manufacturer of that product and ask them to design their product with a little better security in mind.

3.2.1.34 Shut Down system immediately if unable to log security audits: **Not Defined**

One method of obscuring detection in the Security Event Log is to fill the log with so many events that they eventually overwrite one another, or the log fills to capacity, and can't log any more events. The defense against these tactics requires that the computer be disabled (blue-screen) if it is unable to record security events. The local Administrator will still be able to log on at the console, but the machine will not otherwise be usable until the security log is cleared (and preferably archived) and rebooted.

Note: Unless the log is set to "clear manually" or "Overwrite after *x* days" this setting will have no effect. It does emphasize that some care must be taken to maintain the event logs of all Windows machines, including Windows 2000 Professional.

3.2.1.35 Smart Card Removal Behavior: **"Lock Workstation"** (minimum)

In an environment that requires physical logon tokens, or "Smart Cards", one question that inevitably must be answered is "What action should be taken when a user leaves his workstation, and takes his Smart Card with him? The choices are "No Action", "Lock Workstation", or "Force Logoff". The purpose of this setting is to keep users honest. Any setting other than "No Action" is acceptable.

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

3.2.1.36 Strengthen Default Permissions of Global System Objects (e.g. Symbolic Links): **Enabled**

Windows 2000 keeps a list of shared objects and their default Access Control Lists. The "strengthened" setting for these Access Control Lists allow users read access to all users' shared objects, and full access to their own.

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

3.2.1.37 Unsigned Driver Installation Behavior: **"Warn, but allow installation"** (minimum) or **"Do Not Allow Installation"**.

Microsoft has generally shipped drivers with a digital signature, expressing that Microsoft itself has certified the drivers as valid, and tested not to perform actions that constitute foul play. Unfortunately, not all drivers (even from Microsoft) are distributed with digital signatures. These settings should be set to anything other than silent success. If a user or administrator attempts to install unauthenticated drivers, they should at least receive a warning against such action. This setting should read "Warn, but allow installation" or "Do Not Allow Installation".

3.2.1.38 Unsigned Non-Driver Installation Behavior: **"Warn, but allow installation"** (minimum) or **"Do Not Allow Installation"**.

Much like the setting above, not all software installed from Microsoft or anyone else is guaranteed to include the requisite digital signature. It is still important to alert the user that software is being installed on their system, and give them the opportunity to abort the installation. Set this to "Warn, but allow installation" or "Do Not Allow Installation".

WARNING: It is important to understand that forcing users to acknowledge the installation of any software that does not include a digital signature will probably require a significant amount of user education, and you can expect some level of help desk support. Users will be calling in to report that (among other things) many Microsoft hotfixes are not digitally signed.

3.2.2 Additional Registry Settings

The following paragraphs describe individual security settings that can be applied in a variety of ways – using REGEDIT.EXE, REGEDT32.EXE, Local Group Policy, or Domain Group Policy. For more information on applying changes directly to a Windows 2000 Professional registry, please consult the Microsoft TechNet Internet site at http://www.microsoft.com/technet. Some other helpful registry information is available at http://support.microsoft.com/default.aspx?scid=kb;en-us;Q256986 and http://www.microsoft.com/technet/prodtechnol/winntas/tips/winntmag/inreg.asp.

WARNING: Editing the registry can make a system unbootable and unusable if done improperly. If you are not familiar with editing the registry, please take a few minutes and follow the links to Microsoft's TechNet resources, and learn about some of the precautions you should take before editing the registry.

3.2.2.1 Suppress Dr. Watson Crash Dumps: **HKLM\Software\Microsoft\DrWatson\ CreateCrashDump (REG_DWORD) 0**

Dr. Watson is one of Microsoft's utilities that handles errors in applications. If an application produces an error that Dr. Watson can manage, it will dump the contents of memory for that application to a file for future analysis.

In the process of writing the contents of memory to disk, it is entirely possible that password information could be written to disk as well, and later exploited. Set this value to zero to prevent Dr. Watson from writing crash dumps to disk.

3.2.2.2 Disable Automatic Execution of the System Debugger: **HKLM\Software\Microsoft\Windows NT\CurrentVersion\AEDebug\Auto (REG_DWORD) 0**

If an application is executed in non-privileged memory, and the system debugger is started, it is possible for that application to execute code in privileged memory space. Set this value to zero to prevent the system debugger from executing automatically.

3.2.2.3 Disable autoplay from any disk type, regardless of application: **HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun (REG_DWORD) 255**

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.

3.2.2.3.1 Disable autoplay for the current user: **HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun (REG_DWORD) 255**

Note: Due to the inability to manage registry entries for each local user via Security Templates, this setting is recommended, but not required or measured.

3.2.2.3.2 Disable autoplay for all disks when no users are logged on (setting removed): **HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer\NoDriveTypeAutoRun (REG_DWORD) Not Defined**

3.2.2.4 Disable Automatic Logon: **HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon (REG_SZ) 0**

Windows also has the ability to automatically log a user on every time that machine starts up. Some users may prefer this as a feature. Some server based applications may require that a user log in before they can execute, so they require this activity as well.

The problem with this "feature" is that in order for it to work, it stores the username and password for that user in plaintext in the registry. Set this value to zero to prevent any user from automatically logging in when the computer starts up.

3.2.2.5 Don't display username of last successful logon at the logon screen: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName (REG_SZ) Not Defined**

One of the default features of Windows is that if you log off a Windows computer, when you press CTRL+ALT+Delete to log back on, it remembers your username, and you only have to type your password to log back on.

Unfortunately, this terribly convenient feature can also be used by anyone who can press the CTRL+ALT+Delete keys to obtain a valid username for your machine. Setting this value to "1" (as a string) prevents the casual observer from discovering your username.

NOTE: This does not protect a computer from any network based name enumeration, only from the casual observer.

NOTE: This setting is redundant with item 3.2.1.15 and will not be included in future versions of this benchmark.

3.2.2.6 Disable System File Checker Popups: **HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable (REG_DWORD)** ***Not Defined***

Note: Due to the processor-intensive nature of the System File Checker, it is no longer required on startup.

3.2.2.7 Enable the System File Checker to verify all operating system files at boot time: **HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCScan (REG_DWORD)** ***Not Defined***

Note: Due to the processor-intensive nature of the System File Checker, it is no longer required on startup.

3.2.2.8 Do not show the System File Checker progress meter: **HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCShowProgress (REG_DWORD)** ***Not Defined***

Note: Due to the processor-intensive nature of the System File Checker, it is no longer required on startup.

3.2.2.9 Disable automatic reboots after a Blue Screen of Death: **HKLM\System\CurrentControlSet\Control\CrashControl\AutoReboot (REG_DWORD) 0**

If someone manages to get enough control of your computer that they can plant an application there, the next step is to force your computer to restart to register that app. One easy way to accomplish this task is to programmatically force an error that causes the computer to crash, or "Blue Screen" which will reboot the machine by default. Set this Value to zero to prevent this behavior from happening, and at least alert the user that something is wrong.

3.2.2.10 Disable CD Autorun: **HKLM\System\CurrentControlSet\Services\CDrom\Autorun (REG_DWORD) 0**

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.

3.2.2.11 Remove administrative shares on workstation (Professional): **HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks (REG_DWORD) 0**

Every Windows NT/2000 computer automatically has "Administrative Shares" installed by default. These are restricted to use by Administrators, but they expose each volume root, and the %systemroot% folder to the network as Admin$, C$, etc. These make remote administration convenient, but they also present a risk if someone manages to guess the password to an administrative account.

WARNING: If you use administrative shares on your network for remote backups, antivirus support, or general remote administration, this will break your applications. Please ask your software vendors to design around this requirement in future versions of their applications.

3.2.2.12 Protect against Computer Browser Spoofing Attacks: **HKLM\System\CurrentControlSet\Services\MrxSmb\Parameters\RefuseReset (REG_DWORD) 1**

Although this standard advises end-users to shut down their Computer Browser service, it is also likely that not everyone will be able or willing to do so. This registry setting provides protection against a vulnerability that allows the Computer Browse to be shut down. Set this value, to protect against this specific vulnerability. If you are not running the Computer Browser service, this setting will have no effect. More information is available at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q262694.

3.2.2.13 Protect against source-routing spoofing: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting (REG_DWORD) 2**

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.

3.2.2.14 Protect the Default Gateway network setting: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect (REG_DWORD) 0**

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.

3.2.2.15 Ensure ICMP Routing via shortest path first: **HKLM\System\CurrentControlSet\Services\Tcpip\ Parameters\EnableICMPRedirect (REG_DWORD) 0**

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. For more information, please refer to the Microsoft article at http://support.microsoft.com/default.aspx?scid=kb;EN-US;q293626.

3.2.2.16 Help protect against packet fragmentation: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery (REG_DWORD) 0**

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.

Set this value to 0 to force Windows to use a consistent 576 byte packet. More details are available at http://support.microsoft.com/?kbid=315669.

3.2.2.17 Manage Keep-alive times: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime (REG_DWORD) 300000**

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.

3.2.2.18 Protect Against Malicious Name-Release Attacks: **HKLM\System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand (REG_DWORD) 1**

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.

3.2.2.19 Ensure Router Discovery is Disabled: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery (REG_DWORD) 0**

3.2.2.20 Protect against SYN Flood attacks: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect (REG_DWORD) 2**

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.

3.2.2.21 SYN Attack protection – Manage TCP Maximum half-open sockets: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen (REG_DWORD) 100**

This value determines how many incomplete handshake requests the network will allow at one time. This provides protection if SynAttackProtect is set to 1. 100 is the default value on Windows 2000 Professional.

3.2.2.22 SYN Attack protection – Manage TCP Maximum half-open retired sockets: **HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetired (REG_DWORD) 80**

This value indicates how many retransmitted SYN sessions are permitted. The Default value is 80 for Windows 2000 Professional.

3.2.2.23 Enable IPSec to protect Kerberos RSVP Traffic: **HKLM\System\CurrentControlSet\Services\IPSEC\NoDefaultExempt (REG_DWORD) 1**

When Kerberos authentication information is transferred between domain controllers, or between domain controllers and member servers or workstations, it is not secured by default.

Even when IPSec is used to encrypt that traffic, the Kerberos information is considered "exempt". Set this value to 1 to ensure that all traffic, including Kerberos information is protected by IPSec.

3.2.2.24 Do not announce this computer to domain master browsers: **HKLM\System\CurrentControlSet\Services\Lanmanserver\Parameters\Hidden (REG_DWORD) 1**

If the Computer Browser service is disabled, or if this computer is not part of a domain, this setting has no effect. Otherwise, it will prevent the computer from announcing itself to the browser services of other computers, and only act as a "listener" on domain browse lists.

WARNING: This setting will remove your computer from the list of available computers in your domain in Network Neighborhood. This should already be done by disabling the Computer Browser service, but this setting will perform the same function.

4 Additional Security Protection

Many of the previous security related settings 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". These services are scheduled to start either at boot time, as normal Automatic or Manual startup, or disabled to not start at all.

The services listed below should be disabled to protect your computer against certain vulnerabilities. These services may also restrict certain functionality that you are accustomed to, but we have tried to maintain a reasonable level of functionality where possible.

Permissions on services listed here: **Administrators: Full Control; System: Read, Start, Stop, and Pause.** Permissions on services should be set using the Security template that accompanies the CIS Windows Scoring Tool.

4.1.1 Alerter – **Disabled**

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.

4.1.2 Clipbook – **Disabled**

The Clipbook service is used to share clipboard information between computers on a network. In most cases, users don't want to share that information with other computers.

4.1.3 Computer Browser – **Disabled**

The Computer Browser (not to be confused with Internet browsers, such as Internet Explorer or Netscape) keeps track of the computers on a network within a domain. It allows

users to "browse" through Network Neighborhood to find the shared resources they need without knowing the exact name of that resource.

Unfortunately, it allows anyone to browse to those resources before checking any sort of authentication or authorization.

Disabling this service will require users to know the resources they are looking for, by name, and may result in an increased number of help desk calls.

4.1.4 Fax Service – **Disabled**

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.

4.1.5 FTP Publishing Service – **Disabled**

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.

4.1.6 IIS Admin Service – **Disabled**

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.

4.1.7 Internet Connection Sharing – **Disabled**

One of the features introduced with Windows 2000 was the idea of Internet Connection Sharing (ICS) – that is allowing one computer to connect to the Internet and act as a gateway, while allowing other connected computers to access the Internet through that connection.

ICS should not be installed on most computers. If it is, it should be configured properly and securely, which is beyond the scope of this benchmark. If it is installed, regardless of whether or not it is done properly, there is a level of risk involved with its presence.

4.1.8 Messenger – **Disabled**

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.

4.1.9 NetMeeting Remote Desktop Sharing – **Disabled**

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.

4.1.10 Remote Registry Service – **Disabled**

The Windows Registry is essentially a database of settings and configuration options that affect almost every function of a Windows 2000 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.

4.1.11 Routing and Remote Access – **Disabled**

The Routing and Remote Access service is normally used either to facilitate servers are Remote Access Servers, or to allow computers from one network to interact with computers on another.

RRAS is not fully implemented on Windows 2000 Professional like it is in the server operating systems. Users generally don't need RRAS on workstations. If this service can not be disabled, it should be locked down as much as possible. More information is available at http://www.microsoft.com/TechNet/columns/cableguy/cg0601.asp.

4.1.12 Simple Mail Transfer Protocol (SMTP) – **Disabled**

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.

4.1.13 Simple Network Management Protocol (SNMP) Service – **Disabled**

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.

4.1.14 Simple Network Management Protocol (SNMP) Trap – **Disabled**

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

4.1.15 Telnet – **Disabled**

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.

4.1.16 World Wide Web Publishing Services – **Disabled**

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.

4.1.17 Automatic Updates – **Not Defined**

The Automatic Updates service is new to Windows 2000 Service Pack 3. It continually checks the Microsoft web site in the background, and initiates the download of any new Critical Updates as they become available. It is designed to NOT use excessive network bandwidth. This service does not install anything itself, it makes updates ready to install.

NOTE: The Automatic Updates service and the Background Intelligent Transfer Service work together to help keep computers up to date with the latest critical patches. Organizations which have a separate patch management strategy should disable these services to prevent unmanaged system patching. Other organizations or individual users that do not have another method of patching should leave these services enabled and make use of this gift from Microsoft to keep patches up to date.

4.1.18 Background Intelligent Transfer Service (a.k.a. BITS) – **Not Defined**

The BITS service works in conjunction with the Automatic Updates service to download Critical Updates from Microsoft's Internet site, and make them available for installation. The service runs in the background, and makes use of unused and available bandwidth.

4.2 User Rights

In conjunction with many of the privileged groups in Windows 2000, there are a number of individual rights that can be assigned to users or groups to grant them abilities that would be beyond the reach of normal users. Not all of these rights apply to Windows 2000 Professional, but many do.

4.2.1 Access this computer from the network: **Users, Administrators (or none)**

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: **None**

The operating system works in a special security context called "LocalSystem". This security context has the ability to do things that 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: **Not applicable**

This user right only applies to domain controllers, and has no effect on Windows 2000 Professional.

4.2.4 Back up files and directories: **Administrators**

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. It should be restricted when possible.

4.2.5 Bypass traverse checking: **Users**

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.

4.2.6 Change the system time: **Administrators**

Changing the system time on Windows 2000 computers is especially important to restrict in a domain environment because of the role that time synchronization plays in Kerberos authentication. This should not be configurable to anyone except Administrators.

4.2.7 Create a pagefile: **Administrators**

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

4.2.8 Create a token object: **None**

Allows the creation of a security access token. This right should never be given to any user.

4.2.9 Create permanent shared objects: **None**

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.

4.2.10 Debug Programs: **None**

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.

4.2.11 Deny access to this computer from the network: **Guests**

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.

4.2.12 Deny logon as a batch job: **None by default (others allowable as appropriate)**

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.

4.2.13 Deny logon as a service: **None by default (others allowable as appropriate)**

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.

4.2.14 Deny logon locally: **None by default (others allowable as appropriate)**

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.

4.2.15 Enable computer and user accounts to be trusted for delegation: **Not Applicable**

This user right only applies to Windows 2000 Domain Controllers. It has no effect on Windows 2000 Professional.

4.2.16 Force shutdown from a remote system: **Administrators**

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.

4.2.17 Generate security audits: **None**

This user right allows a user or process to generate events to be added to the Windows Security Event Log. This right should not be granted to any user or group.

4.2.18 Increase quotas: **Administrators**

The right to increase quotas applies to one process manipulating the processor quota of another process. This can be used in performance tuning, but can also cause a denial of service attack if misused or abused.

4.2.19 Increase scheduling priority: **Administrators**

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.

4.2.20 Load and unload device drivers: **Administrators**

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.

4.2.21 Lock pages in memory: **None**

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.

4.2.22 Log on as a batch job: **None**

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.

4.2.23 Log on as a service: **None**

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 LocalSystem

security credentials. If a service needs to be executed in a user context, that user would have to be listed here.

4.2.24 Log on locally: **Users, Administrators (further restriction allowable)**

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

4.2.25 Manage auditing and security log: **Administrators**

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.

4.2.26 Modify firmware environment values: **Administrators**

Individual users have the ability to change their own environment variables, but only Administrators and accounts that hold this right can change the environment variables of other users on a system.

4.2.27 Profile single process: **Administrators**

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

4.2.28 Profile system performance: **Administrators**

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

4.2.29 Remove computer from docking station: **Users, Administrators**

This user right is just what you'd expect.

4.2.30 Replace a process level token: **None**

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

4.2.31 Restore files and directories: **Administrators**

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. It should be restricted to Administrators.

4.2.32 Shut down the system: **Users, Administrators**

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.

4.2.33 Synchronize directory service data: **Not Applicable**

This user right has no effect on Windows 2000 Professional.

4.2.34 Take ownership of file or other objects: **Administrators**

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 – that is if you have the option of booting into Windows 2000 or Windows 9x. 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.

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.

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

* Unless stated otherwise, Administrators or System Full Control is full control for the designated folder and all contents. Creator Owner Full Control is for subfolders and files only. Users permissions are for current folder, subfolders, and files. Files listed with an "a.k.a." may be listed on "%SystemDrive%" or on "C:\", so both entries are included in the accompanying template.

4.4.1.1 %SystemDrive%\ - **Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List**

4.4.1.2 %SystemDrive%\autoexec.bat (a.k.a. – c:\autoexec.bat) – **Administrators: Full; System: Full**

4.4.1.3 %SystemDrive%\boot.ini (a.k.a. – c:\boot.ini) – **Administrators: Full; System: Full**

4.4.1.4 %SystemDrive%\config.sys (a.k.a. – c:\config.sys) - **Administrators: Full; System: Full**

4.4.1.5 %SystemDrive%\io.sys – **Administrators: Full; System: Full**

4.4.1.6 %SystemDrive%\msdos.sys – **Administrators: Full; System: Full**

4.4.1.7 %SystemDrive%\ntbootdd.sys - (a.k.a. – c:\ntbootdd.sys) **Administrators: Full; System: Full**

4.4.1.8 %SystemDrive%\ntdetect.com – **Administrators: Full; System: Full**

4.4.1.9 %SystemDrive%\ntldr - **Administrators: Full; System: Full**

4.4.1.10 %SystemDrive%\Documents and Settings – **Administrators: Full; System: Full; Users: Read and Execute, List**

4.4.1.11 %SystemDrive%\Documents and Settings\Administrator – **Administrators: Full; System: Full**

4.4.1.12 %SystemDrive%\Documents and Settings\All Users – **Administrators: Full; System: Full; Users: Read and Execute, List**

4.4.1.13 %SystemDrive%\Documents and Settings\All Users\Documents \DrWatson – **Administrators: Full; System: Full; Creator Owner: Full; Users: Traverse Folder/Execute File, List Folder/Read Data, Read Attributes, Read Extended Attributes, Read Permissions (This folder, subfolders, and files); Users: Traverse Folder/Execute Files, Create Files/Write Data, Create Folder/Append Data (Subfolders and files only)**

4.4.1.14 %SystemDrive%\Documents and Settings\Default User – **Administrators: Full; System: Full; Users: Read and Execute, List**

4.4.1.15 %ProgramFiles% - **Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List**

4.4.1.16 %Program Files%\Resource Kit – **Administrators: Full; System: Full**

4.4.1.17 %Program Files%\Resource Pro Kit – **Administrators: Full; System: Full**

4.4.1.18 %SystemRoot% – **Administrators: Full; System: Full; Creator Onwer: Full; Users: Read and Execute, List**

4.4.1.19 %SystemRoot%\$NtServicePackUninstall$ – **Administrators: Full; System: Full**

4.4.1.20 %SystemRoot%\CSC – **Administrators: Full; System: Full**

4.4.1.21 %SystemRoot%\Debug - **Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List**

4.4.1.22 %SystemRoot%\Debug\UserMode - **Administrators: Full; System: Full; Users: Traverse Folder/Execute File, List folder/Read data, Create files/Write data (This folder, only); Create files/Write data, Create folders/Append data (Files only)**

4.4.1.23 %SystemRoot%\Offline Web Pages – **Ignore Parent Permission Changes**

4.4.1.24 %SystemRoot%\Registration - **Administrators: Full; System: Full; Users: Read**

4.4.1.25 %SystemRoot%\repair - **Administrators: Full; System: Full**

4.4.1.26 %SystemRoot%\security - **Administrators: Full; System: Full; Creator Owner: Full**

4.4.1.27 %SystemRoot%\system32 - **Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List**

4.4.1.28 %SystemRoot%\system32\at.exe – **Administrators: Full; System: Full**

4.4.1.29 %SystemRoot%\system32\Ntbackup.exe – **Administrators: Full; System: Full**

4.4.1.30 %SystemRoot%\system32\rcp.exe – **Administrators: Full; System: Full**

4.4.1.31 %SystemRoot%\regedit.exe – **Administrators: Full; System: Full**

4.4.1.32 %SystemRoot%\system32\regedt32.exe – **Administrators: Full; System: Full**

4.4.1.33 %SystemRoot%\system32\rexec.exe – **Administrators: Full; System: Full**

4.4.1.34 %SystemRoot%\system32\rsh.exe – **Administrators: Full; System: Full**

4.4.1.35 %SystemRoot%\system32\secedit.exe – **Administrators: Full; System: Full**

4.4.1.36 %SystemRoot%\system32\appmgmt – **Administrators: Full; System: Full; Users: Read and Execute, List**

4.4.1.37 %SystemRoot%\system32\config – **Administrators: Full; System: Full**

4.4.1.38 %SystemRoot%\system32\dllcache – **Administrators: Full; System: Full; Creator Owner: Full**

4.4.1.39 %SystemRoot%\system32\DTCLog - **Administrators: Full; System: Full; Creator Owner: Full; Users: Read and Execute, List**

4.4.1.40 %SystemRoot%\system32\Group Policy - **Administrators: Full; System: Full; Authenticated Users: Read and Execute, List**

4.4.1.41 %SystemRoot%\system32\ias - **Administrators: Full; System: Full; Creator Owner: Full**

4.4.1.42 %SystemRoot%\system32\NTMSData – **Administrators: Full; System: Full**

4.4.1.43 %SystemRoot%\system32\reinstallbackups – **Administrators: Full; System: Full; Creator Owner: Full; Power Users: Read and Execute, List**

4.4.1.44 %SystemRoot%\system32\Setup – **Administrators: Full; System: Full; Users: Read and Execute, List**

4.4.1.45 %SystemRoot%\system32\spool\printers – **Administrators: Full; System: Full; Creator Owner: Full; Users: Traverse Folder, Execute File, Read, Read Extended Attributes, Create folders, Append Data**

4.4.1.46 %SystemRoot%\Tasks - **(Do not allow permissions on this folder to be replaced)**

4.4.1.47 %SystemDrive%\System Volume Information – **(Do not allow permissions on this folder to be replaced)**

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\Classes - **Administrators: Full; System: Full; Creator Owner: Full; Users: Read**

4.4.2.2 HKLM\Software – **Administrators Full; System: Full; Creator Owner: Full; Users: Read**

4.4.2.3 HKLM\Software\Microsoft\Net DDE – **Administrators: Full; System: Full**

4.4.2.4 HKLM\Software\Microsoft\OS/2 Subsystem for NT – **Administrators: Full; System: Full; Creator Owner: Full**

4.4.2.5 HKLM\Software\Microsoft\Windows NT\CurrentVersion\AsrCommands – **Administrators: Full; System: Full; Creator Owner: Full; Users: Read; Backup Operators: Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, Read (this key and subkeys)**

4.4.2.6 HKLM\Software\Microsoft\Windows NT\CurrentVersion\Perflib – **Administrators: Full; System: Full; Creator Owner: Full; Interactive: Read (this key and subkeys)**

4.4.2.7 HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy - **Administrators: Full; System: Full; Authenticated Users: Read**

4.4.2.8 HKLM\Software\Microsoft\Windows\CurrentVersion\Installer - **Administrators Full; System: Full; Users: Read**

4.4.2.9 HKLM\Software\Microsoft\Windows\CurrentVersion\Policies - **Administrators: Full; System: Full; Authenticated Users: Read**

4.4.2.10 HKLM\System - **Administrators Full; System: Full; Creator Owner: Full; Users: Read**

4.4.2.11 HKLM\System\Clone – **Allow inheritable permissions to propagate to this object**

4.4.2.12 HKLM\System\ControlSet001 - **Administrators Full; System: Full; Creator Owner: Full; Users: Read**

4.4.2.13 HKLM\System\ControlSet00x - **Administrators Full; System: Full; Creator Owner: Full; Users: Read**

* Apply these permissions to all control sets other than CurrentControlSet.

4.4.2.14 HKLM\System\CurrentControlSet\Control\SecurePipeServers\WinReg – **Administrators: Full**

4.4.2.15 HKLM\System\CurrentControlSet\Control\WMI\Security – **Administrators: Full; System: Full; Creator Owner: Full**

4.4.2.16 HKLM\System\CurrentControlSet\Enum - **(Do not allow permissions on this folder to be replaced)**

4.4.2.17 HKLM\System\CurrentControlSet\Hardware Profiles – **Administrators Full; System: Full; Creator Owner: Full; Users: Read**

4.4.2.18 HKLM\System\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers - **Administrators Full; System: Full; Creator Owner: Full**

4.4.2.19 HKLM\System\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities - **Administrators Full; System: Full; Creator Owner: Full**

4.4.2.20 HKU\.Default - **Administrators Full; System: Full; Creator Owner: Full; Users: Read**

4.4.2.21 HKU\.Default\Software\Microsoft\NetDDE - **Administrators Full; System: Full**

4.4.2.22 HKU\.Default\Software\Microsoft\Protected Storage System Provider – **No entries**

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.

4.4.3.1 %SystemDrive% - **Everyone: Failures (this folder, propagate inheritable permissions to all subfolders and files)**

4.4.3.2 HKLM\Software – **Everyone: Failures (this key, propagate inheritable permission to all subkeys)**

4.4.3.3 HKLM\System – **Everyone: Failures (this key, propagate inheritable permission to all subkeys)**

Appendix A: Windows Security Questionnaire

The Windows 2000 Professional Security Benchmarks represent a general consensus of steps that can be taken to allow most of the normal functionality of a Windows 2000 Professional computer, while mitigating many common Internet risks. These settings have been presented in Section 1, and then described in greater detail in Section 2. These two sections together constitute the CIS Windows 2000 Professional Security Benchmark.

In addition to the configurations described above, there is a great deal more that can be done, depending on what role your computer fulfills, and what type of computer environment you are in. Well managed environments that have full time computer security support professionals may not have a great deal of need for this appendix, but there are a great many businesses, with or without dedicated personnel, who may be able to protect themselves better with help from this question-and-answer session.

1. **Does anyone on another computer use shared files or printers from your computer?**

   Yes: Your Windows 2000 Professional computer is already capable of sharing files and printers with other computers on your network.

   Do This: Go on to the next question.

   No: In addition to the steps already taken, you can DISABLE file and printer sharing and deny remote access to your computer entirely!

   Do This: Disable File and Printer Sharing:
   - Click Start -> Settings -> Network and Dial-Up Connections.
   - Right-click each active connection, and click Properties.
   - Un-check the box for "File and Printer Sharing for Microsoft Networks".
   - Click OK.

   Do This: Deny all access from Network users:
   - Click Start -> Settings -> Control Panel.
   - Double-click Administrative Tools.
   - Double-click Local Security Policy.
   - Navigate to Local Policies -> User Rights Assignment.
   - Double-click "Deny Access to this computer from the network".
   - Click Add.
   - Double-click "Everyone" and click OK.
   - Click OK again, and close all open windows.

2. **Does your computer use resources (files or printers) stored on any other computers on your network, other than Internet mail or Internet Browsing?**

   Yes: Your Windows 2000 Professional computer is already capable of sharing files and printers with other computers on your network.

No: In addition to the steps already taken, you can DISABLE all Microsoft networking and deny remote access to your computer entirely!

Do This: Disable Microsoft Networking

- Click Start -> Settings -> Network and Dial-Up Connections.
- Right-click each active connection, and click Properties.
- Un-check the box for “Client for Microsoft Networks”.
- Click OK.

Appendix B: 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

Service Pack 2 Information - http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/

Current Critical Hotfixes - http://www.microsoft.com/windows2000/downloads/critical/

Microsoft Directory Services Client for Windows 9x/Me - http://www.microsoft.com/TechNet/prodtechnol/ntwrkstn/downloads/utils/dsclient.asp?frame=true

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/treeview/default.asp?url=/technet/prodtechnol/winntas/tips/winntmag/inreg.asp

NIST Windows 2000 Security Guidelines - http://csrc.nist.gov/itsec/guidance_W2Kpro.html

Appendix C: Variances from the Consensus Baseline Security Settings for Windows 2000 Professional

Description	Consensus	Benchmark	Reason
Audit the access of global system objects.	Disabled	Not Defined	This generates a large number of events, but can be of benefit if users take the time to analyze event logs. Enabling it should be an option.
Audit use of the Backup and Restore privilege	Disabled	Not Defined	This generates a large number of events, but can be of benefit if users take the time to analyze event logs. Enabling it should be an option.
Restricted Groups:	Power Users	(none)	The restriction of the Power Users group to no users only makes sense if the Administrators can also be limited. Restrict either or both of these groups if it makes sense in customized environments.
HKLM\Software\ Microsoft\ Command Processor\ PathCompletionChar	(REG_ DWORD) 9	Not defined (not listed)	The practice of setting the PathCompletionChar to the Tab key is a good one, but it is not a “security setting”.
Task Scheduler Service	Disabled	Not Defined	The Windows 2000 Task Scheduler is significantly stronger than the same service under Windows NT, and can be used to add to the security of a computer. Individual tasks run under the context of an authorized user account. If used properly, it can enhance the security of a computer.

Appendix D: Problematic Settings

In the course of developing any type of security standard, there is one perpetual constant: Something will be broken. When you change something in favor of increasing security, you are "breaking" a potentially vulnerable or exploitable program.

An unfortunate side-effect of disabling the unwanted services is the likelihood that some hazardous program or function has also been used for good instead of evil. The unfortunate part is that when you disable the risky code, a perfectly viable operation is also disabled.

In an effort to disclose likely sources of problems, this appendix lists some of the settings that are known to cause problems, and what types of problems may arise. This is not an all-inclusive list. It is provided in good faith to help you diagnose problems when securing systems. It is subject to change as information becomes available.

3.1.1: Additional Restrictions for Anonymous connections "No Access Without Explicit Anonymous Permissions". Many older applications (and some new ones) actually use Null Sessions to communicate between computers, or between processes on the same computer. If an application fails to work once a computer is "locked down" this should be the first setting to "undo" while troubleshooting.

3.2.1.16: Lan Manager Authentication Level set to "Send NTLMv2 response only". This setting will make a Windows 2000 computer unable to share resources with other computers that are not set to use NTLMv2. It will make the computer unable to share resources with Windows 95/98/Me computers unless they install the DSCLIENT.EXE application from the Windows 2000 installation CD.

3.2.1.27: Restrict CD-ROM Access to Locally Logged-On User Only. One problem has been identified when this setting is enabled. When users are installing software from a CD-ROM drive, and those installation packages use the Microsoft Installer (.MSI) packages, the software is actually installed by the Windows Installer service, NOT the local 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.

3.2.2.11: Remove administrative shares on workstation (Professional): **HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks (REG_DWORD) 0.** Removing administrative shares on Windows computers is entirely desirable if they are not going to be used. This is likely to break some applications that use administrative shares – the most notable of which are backup and restore utilities.

4.4: File and Registry Permissions. It should go without saying that if a user or application is attempting to access an object, and receiving an "Access Denied" error, that some attention should be paid to the permissions applied to that object.

Appendix E: Change History

July 17, 2002 – Version 1.0 released to public.

September 2, 2002 – Changed 4.4.2.15 to grant Full permissions to Administrators.

Added items 3.2.2.3.1 and 3.2.2.3.2 to compliment NoDriveTypeAutoRun value.

September 13, 2002 – Added Federal Government Terms Of Use Agreement.

October 4, 2002 – Version 2.0 Released.
System File Checker (3.2.2.7) no longer required to run on startup.
Added section (4.4.3) on File and Registry Auditing and their requirements.
Set LAN Manager Authentication to require NTLMv2 (3.2.1.16).

October 18, 2002 – Version 2.0.1 Released.
Corrected template for LAN Manager Authentication setting (3.2.1.16).
Changed file and registry auditing to only audit failures as a minimum setting.
"Appendix D: Problematic Settings" added to benchmark document.

October 25, 2002 – Version 2.0.2 Released.
Remaining SFC registry entries removed from requirements.
Warning added for setting 3.2.1.27 – Restrict CD-ROM Access to Local User Only.

November 4, 2002 – Version 2.0.3 Released.
Corrected setting 3.2.1.4 to comply with Consensus Baseline Standard.
Setting 3.2.1.32 left Not Defined due to conflicts between NT 4.0 and Win2k Domains.
Setting 3.2.1.34 left Not Defined since it is ineffective with the other Event Log settings.
Aliased settings 4.4.1.2, 4.4.1.3, 4.4.1.4, and 4.4.1.7 for systems with multiple drives.

August 13, 2003 – Version 2.0.4 Released.
Modified to reflect new Terms of Use.

September 2, 2003 – Version 2.0.5 Released.
Fixed description of 4.1.6 IIS Admin service.
Changed registry entry 3.2.2.5 to reflect Windows 2000 change of registry location.
Changed value of entry at 3.2.2.16 as per http://support.microsoft.com/?kbid=315669.
Corrected accompanying template to reflect proper service security.
Corrected several file and registry permissions in accompanying security template.

April 2, 2004 – Version 2.1 Released.
Obsolete setting 3.2.2.5 changed to "Not Defined".
Changed setting 4.4.2.1 from HKCU to its synonymous setting HKLM\Software\Classes
Changed setting 4.2.15 to "Not Applicable"
Changed setting 4.2.33 to "Not Applicable"
Settings 4.2.12, 4.2.13, and 4.2.14 changed to "Not Defined" to allow users to customize.
Changed setting 3.2.2.3.2 to "Not Defined"

April 16, 2004 – Version 2.1.1 Released.
Updated to reflect Service Pack 4 as current.

October 5, 2004 – Version 2.2 Released.
Corrected path for setting 4.4.1.37.
Corrected spelling of references to TCPMaxHalfOpenRetried.
Changed 3.2.2.5 to "Not Defined". Does not apply to Win2k Professional.
Added setting 4.4.1.47.

November 15, 2004 – Version 2.2.1 Released.
Corrected permissions setting 4.4.1.23.