

SECURING

WINDOWS

2000

STEP BY STEP

*A consensus document by
security professionals from
dozens of user organizations*

SANS INSTITUTE

Version 1.5 JULY 1, 2001

THE SANS INSTITUTE
WINDOWS 2000
SECURITY
STEP BY STEP
A SURVIVAL GUIDE FOR
WINDOWS 2000 SECURITY:

A consensus document by security professionals.

Version 1.5

July 1, 2001

Copyright 2001. The SANS Institute

**No copying, electronic forwarding,
or posting allowed except with
prior written permission.**

*This guide is the joint product of a community of Windows security managers and experts, who have voluntarily shared their experience in this field so that others may benefit. The guide can be used to substantially improve the security of Windows 2000 computers and networks. This first edition of the "Securing Windows 2000 Step by Step Guide" provides a solid foundation for system security in large and small environments. It will be continually revised in response to ongoing input from the security community. **Please send any additions, corrections, or contributions to win2k@sans.org.** Significant contributors will be recognized in future editions.*

Editor for this edition: Jeff Shawgo

William Ahern, BT Syncordia Solutions

John Bambenek, EYT Inc.

Mark Biltz

Jeffrey W. Brown, CISSP

Melissa Brown, Joint Interoperability Test Command, Fort Huachuca

Patrick Chambet, Edelweb

Christopher Davis, University of Texas, McCombs School of Business

Dean Farrington, Wells Fargo

Antonius J. M. Groothuizen, Eftia OSS Solutions Inc.

Timothy P. Hughes, McCurve Inc.

Arvanitis Ioannis, Infosec Command, NACOSA, NATO

Toby Kohlenberg, Intel Corporate Information Security

Sergei Ledovskij

David Lee, Pitney Bowes Inc.

Ferdinand "Butch" Leland, S3Networks, LLC

Paul Lochbihler, Cinnabar Networks Inc.

Les McCarter, MCSE, MCT, MCNE, CNI of TeraBiz

John Millican, New Concept Technologies

Derek P. Milroy, McCurve Inc.

Robert Mincey, Tekinsight Services

Brendan Moon, Compaq Computer Corporation

Jason Morris, Computer Security Analyst/Enthusiast

Zakaria Nabil, CLICKGSM Vodafone Egypt

Hugh Pierce, Applied Research Associates

Jeff Stehlin, Hewlett-Packard

Dennis Taylor, Director of the NASA SEWP Security Center

Tom Yergeau

We also appreciate the work done by Microsoft's security engineers in reviewing the many drafts and suggesting items for inclusion.

Please be aware that applying many of the settings in this guide will disable a great deal of the standard functionality that ships with Windows 2000. In some cases, it may cause instability, or cripple existing systems. Be sure to test all settings in a non-production environment before making any changes to production systems.

Just as Windows 2000 is the next evolution of Windows NT 4.0, this document is built on Securing Windows NT 4.0 Step-by-Step Guide, also produced by The SANS Institute. It was the joint product of Windows security managers and experts who, together, support more than 286,000 users and have more than 380 years of Windows security experience. Those professionals continue to contribute on a regular basis.

One of the great sources of productivity and effectiveness in the community of computer professionals is the willingness of active practitioners to take time from their busy lives to share some of the lessons they have learned and the techniques they have perfected. Much of the sharing takes place through online news groups, through web postings, and through presentations at technical meetings, and those who are able to take the time to scan the newsgroups, surf the web, and attend the meetings often gain measurably from those interactions.

SANS' Step-by-Step series raises information sharing to a new level in which experts share techniques they have found to be effective. They integrate the techniques into a step-by-step plan and then subject the plan, in detail, to the close scrutiny of other experts. The process continues until consensus is reached. This is a difficult undertaking. A large number of people spend a great deal of time making sure the information is useful and correct.

This booklet largely applies to both Windows 2000 Server environments and, almost as importantly, Windows 2000 Professional environments. Since Windows environments are almost universally networked and/or part of a domain, securing individual workstations is as important as securing the servers.

Windows environments are constantly evolving as new applications and users are added, as new threats and responses emerge, as new Hot Fixes and Service Packs are offered, and as new versions are released. Hence no prescription for setting up a secure environment can claim to be a comprehensive and timeless formula for absolute safety.

Yet, every day, thousands of new servers are deployed in sites around the globe. Executives at those sites believe that their system and security administrators are doing what is necessary to establish and maintain security. This booklet is written for those system administrators and security people who are implementing Windows NT/2000 systems and want to have confidence that they are taking steps that most experienced Windows security experts take to establish and strengthen security on their systems.

Though the booklet provides valuable guidance, it is not a text on the subject. Texts provide background on the way Windows 2000 security, cryptography, and other relevant technologies work, and on less sensitive administrative techniques. In addition, the booklet can not replace in-depth training by skilled instructors. Such security training should be mandatory for new Windows system and security administrators where security is important. Furthermore, acting on all the steps in this booklet does not obviate the need for an overall corporate security policy, effective user education, or for monitoring electronic sources of security updates and acting upon the information they provide. The appendix lists the most popular Windows NT/2000 security web sites and mailing lists that are popular sources of new security threats and solutions.

With all that said, what this booklet does do is offer the consensus advice of Windows security experts from diverse Windows NT/2000 user organizations. The steps outlined in this booklet are the actions that they agree are important in securing Windows 2000 servers and workstations at their sites. Since Windows NT and Windows 2000 are invariably installed in a networked environment, with both servers and workstations, it is as important to secure the individual workstations as it is to secure the servers. Furthermore, although detailed instructions are beyond the scope of this document, other (non-Windows NT/2000) platforms that could impact the security of the network should also be audited and secured.

Securing Windows 2000 Step-by-Step parallels the phases of the implementation and operation of a Windows 2000 system. Steps are organized into those phases and each step's description includes some information about the

problem the step is intended to solve, the actions that need to be taken, tips on how to take the action if it is not obvious, and caveats where they add value. Where actions are more appropriate for organizations with extremely critical security requirements, they are noted with the word "Advanced." The primary focus is on servers, connected in networks, with or without domain services, though some recommendations affect workstations, as well.

Except as otherwise stated, all procedures in this booklet assume that one is running Windows 2000 Server or Advanced Server with Service Pack 1 or higher, with access to the Windows 2000 Server Resource Kit, which can be purchased at any bookstore. Further, many of the registry changes described in this booklet do not take effect until after a reboot. Therefore, it is recommended to reboot after editing the registry.

Localized versions of Windows 2000 are generally harder to secure. Fixes and updates typically arrive more slowly, or not at all, for those versions. Therefore, be sure to test any implementations especially carefully if you have to use a localized version of Windows 2000.

FOREWORD

This Document is arranged in order to make use of the common tools and steps used while implementing and securing an installation of Windows 2000 Professional and Server operating systems.

© SANS Institute 2001, All Rights Reserved

Table of Contents

CHAPTER 1 GENERAL SECURITY GUIDELINES

- 1.1 Security Policy and Company Politics.
- 1.2 The “Cost” of Security.
- 1.3 Develop Different Policies for Different Types of Computers.
- 1.4 Enforce the “Least Privilege” Principle.
- 1.5 Avoid Granting Administrator Privileges.
- 1.6 Identify the Owners of Physical and Electronic Property.
- 1.7 Limit Domain Trust.
- 1.8 Restrict Modems in Workstations and Servers.
- 1.9 Limit Access to “Sniffer” software.
- 1.10 Keep Systems Software Up To Date.
- 1.11 Update and Practice a Recovery Plan.
- 1.12 Require Strong Passwords.
- 1.13 Require Password Protected Screen Savers.
- 1.14 Establish Auditing and Review Policies.
- 1.15 Require Administrators to Maintain a User and an Administrator Account.
- 1.16 Create an Administrator Password Control Process.
- 1.17 Require Virus Protection Software.
- 1.18 Recommend Host Based Intrusion Detection Systems (IDS).
- 1.19 Perform Periodical Low-Level Security Audits.
- 1.20 Be Quick to Disable Accounts of Terminated Employees.
- 1.21 Establish and Practice System and Application Recovery Plans.

CHAPTER 2 PHYSICAL DATA SECURITY

- 2.1 Enable the End User to Protect Laptops.
- 2.2 Physically Secure Servers.
- 2.3 Protect the Server from Unattended Reboot.
 - 2.3.1 Protect the SAM with SYSKEY.
- 2.4 Protect the Backup Tapes.
- 2.5 Use NTFS Disk Partitions.
- 2.6 Enable the Encrypting File System.
 - 2.6.1 Using the Encrypting File System on Portable Computers.
 - 2.6.2 Backup the File Encryption Certificate and the associated Private Key.
 - 2.6.3 Recovery Agent Management.
- 2.7 Uninterruptible Power Supplies.
- 2.8 Environmental Protection.
- 2.9 Windows File Protection.

CHAPTER 3 WINDOWS 2000 SECURITY POLICY CONFIGURATION

- 3.1 Configure the Local Security Policy.
 - 3.1.1 Configure the Account Policy.
 - 3.1.1.1 Secure the Administrator and Guest Accounts.
 - 3.1.2 Configure the Local Policies.
 - 3.1.2.1 Enable Audit Policies.
 - 3.1.2.2 Customize User Rights.
 - 3.1.2.3 Customize Security Options.
 - 3.1.2.3.1 Additional Restrictions for Anonymous Connections.
 - 3.1.2.3.2 Allow Server Operators to Schedule Tasks (Domain Controllers Only).

- 3.1.2.3.3 Allow System to be Shut Down Without Having to Log On.
- 3.1.2.3.4 Allowed to Eject Removable NTFS Media.
- 3.1.2.3.5 Amount of Idle Time Required Before Disconnecting Session.
- 3.1.2.3.6 Audit the Access of Global System Objects.
- 3.1.2.3.7 Audit Use of Backup and Restore Privilege.
- 3.1.2.3.8 Automatically Log Off Users When Logon Time Expires (Local).
- 3.1.2.3.9 Clear Virtual Memory Pagefile When System Shuts Down.
- 3.1.2.3.10 Digitally Sign Client Communication (Always/When Possible).
- 3.1.2.3.11 Digitally Sign Server Communication (Always/When Possible).
- 3.1.2.3.12 Disable CTRL+ALT+DEL Requirement for Logon.
- 3.1.2.3.13 Do Not Display Last User Name in Logon Screen.
- 3.1.2.3.14 LAN Manager Authentication Level.
- 3.1.2.3.15 Message Text/Title for users attempting to Logon.
- 3.1.2.3.16 Number of Previous Logons to Cache (If Domain Controller is Not Available).
- 3.1.2.3.17 Prevent System Maintenance of Computer Account Password.
- 3.1.2.3.18 Prevent Users From Installing Print Drivers.
- 3.1.2.3.19 Prompt User to Change Password Before Expiration.
- 3.1.2.3.20 Recovery Console: Allow Automatic Administrative Logon.
- 3.1.2.3.21 Recovery Console: Allow Floppy Copy and Access to All Drives and Folders.
- 3.1.2.3.22 Rename the Administrator and Guest Accounts.
- 3.1.2.3.23 Restrict the CD-ROM and Floppy drive access to locally logged on user only.
- 3.1.2.3.24 Secure the Netlogon Channel.
- 3.1.2.3.25 Send Unencrypted Credentials for Third Party SMB Servers.
- 3.1.2.3.26 Shut Down System Immediately If Unable to Log Security Audits.
- 3.1.2.3.27 Configure Smart Card Removal Behavior.
- 3.1.2.3.28 Strengthen Default Permissions of Global System Objects.
- 3.1.2.3.29 Configure Unsigned Driver Installation Behavior.
- 3.1.2.3.30 Configure Unsigned Non-Driver Installation Behavior.
- 3.1.3 Configure the Public Key Policy.
- 3.1.4 Configure the IP Security Policy.
- 3.2 Group Policy
- 3.3 Computer Management MMC Snap-In
 - 3.3.1 System Tools
 - 3.3.1.1 Configure Event Log Settings.
 - 3.3.1.2 System Information.
 - 3.3.1.3 Performance Logs and Alerts.
 - 3.3.1.4 Shared Folders.
 - 3.3.1.5 Local Users and Groups.
 - 3.3.2 Services and Applications.
 - 3.3.2.1 WMI Control.
 - 3.3.2.2 Services.
 - 3.3.2.3 Indexing Service.
 - 3.3.2.4 SNMP Service.
- 3.4 Additional Recommended Tools and Utilities.
 - 3.4.1 Lock out unauthorized use of the Floppy Drive.
 - 3.4.2 Enable network lockout of the Administrator account.
 - 3.4.3 Allow Windows 95/98/Me to use NTLMv2 in an Active Directory Domain.
- 3.5 Disable Unused Services under Windows 2000.
 - 3.5.1 Remove the OS/2 and Posix Subsystems.
- 3.6 Secure any Remote Control Programs.

- 3.6.1 PC Anywhere.
- 3.6.2 Windows 2000 Terminal Services – Remote Administration.

3.7 Windows 2000 Network Interface – Disable Microsoft Network Client.

CHAPTER 4 ADDITIONAL UTILITIES

4.1 Windows 2000 Support Tools

- 4.1.1 Computer Management Tools.
- 4.1.2 Deployment Tools.
- 4.1.3 Diagnostic Tools.
- 4.1.4 File and Disk Tools.
- 4.1.5 Network Management Tools.
- 4.1.6 Performance Tools.

4.2 Windows 2000 Resource Kit Tools

- 4.2.1 Computer Management Tools
- 4.2.2 Desktop Tools.
- 4.2.3 Diagnostics Tools.
- 4.2.4 File and Disk Tools.
- 4.2.5 Internet Information Services.
- 4.2.6 Network Management Tools.
- 4.2.7 Performance Tools.
- 4.2.8 Scripting Tools.
- 4.2.9 Security Tools.
- 4.2.10 Additional Microsoft and Third Party Applications.

4.3 Freeware, Shareware, and Commercial Tools.

- 4.3.1 Use Access Control List Auditing Tools.
- 4.3.2 Audit Service Pack and HotFix Levels on Windows Machines.
- 4.3.3 User Manager Pro and NT Service Account Manager for Windows NT/2000.
- 4.3.4 Event Log Monitor from TNT Software.
- 4.3.5 EventAdmin from Aelita Software.
- 4.3.6 Nmap.
- 4.3.7 WinDump.
- 4.3.8 PGP Encryption.
- 4.3.9 HFCCheck from Microsoft.
- 4.3.10 Health Monitor 2.1.
- 4.3.11 Atelier Web Security Port Scanner.
- 4.3.12 Anti-Trojan.
- 4.3.13 L0phtCrack 3.
- 4.3.14 ModemSwitcher.
- 4.3.15 Snort.

4.4 Edit the Registry.

- 4.4.1 Disable Autorun on CD-Rom Drives.
- 4.4.2 Controlling Remote Registry Access.
 - 4.4.2.1 Exception to Remote Registry Access.
- 4.4.3 Restrict Null User access to Named Pipes.
- 4.4.4 Restrict Null User access to Shares.
- 4.4.5 Mitigate the Risk of Syn Flood Attacks.
- 4.4.6 Disable Router Discovery.
- 4.4.7 Disable IP Source Routing.
- 4.4.8 Tune the TCP/IP KeepAlive Timer.
- 4.4.9 Disable ICMP Redirects.
- 4.4.10 Disable External Name Release.

- 4.4.11 Disable DCOM.
- 4.4.12 Remove Administrative Shares.
- 4.4.13 Disable 8.3 Filename Creation.

CHAPTER 5 FILE, FOLDER, AND REGISTRY PERMISSIONS

- 5.1 Setting Permissions Easily.
- 5.2 File and Folder Permissions.
- 5.3 Registry Key Permissions.

CHAPTER 6 WINDOWS 2000 SECURITY CONFIGURATION AND ANALYSIS TOOL

- 6.1 Applying Standard Incremental Windows 2000 Security Templates.
- 6.2 Creating Custom Policies with the Security Configuration and Analysis Tool.
- 6.3 Default Windows 2000 Security Templates.
- 6.4 Performing Analysis of a Computer.
- 6.5 Command-Line Configuration and Analysis.
- 6.6 Security Template Tips.

CHAPTER 7 WINDOWS 2000 RECOVERY OPTIONS

- 7.1 Windows 2000 Backups.
 - 7.1.1 Baseline System Backup.
 - 7.1.2 Regular System Backups.
 - 7.1.3 Remote System Backups.
 - 7.1.4 NTBackup.exe – Command Line Options.
- 7.2 Emergency Repair Disks.
- 7.3 Windows 2000 Backup System Security Measures.
- 7.4 Safe Mode.
- 7.5 Safe Mode with Networking.
- 7.6 Safe Mode with Command Prompt.
- 7.7 Recovery Console.

CHAPTER 8 WINDOWS 2000 DOMAINS: ACTIVE DIRECTORY SERVICES

- 8.1 Domain Controllers.
- 8.2 Trust.
- 8.3 Look at the trees, but see the forest.
- 8.4 Enterprise Administrator and Schema Admins.

CHAPTER 9 WINDOWS 2000 APPLICATION SECURITY

- 9.1 Internet Information Services 5.
- 9.2 Telnet Server.
- 9.3 File and Printer Sharing.
- 9.4 Microsoft Windows Services For Unix 2.0.
- 9.5 Microsoft Exchange, Outlook, and Outlook Express.
- 9.6 Microsoft SQL Server.
- 9.7 Terminal Services Application Server

APPENDIX A USEFUL WEB SITES AND MAILING LISTS

APPENDIX B WINDOWS 2000 SECURITY CHECKLIST

APPENDIX C CHANGE HISTORY

CHAPTER 1 GENERAL SECURITY GUIDELINES

1.1 Security Policy and Company Politics.

In a perfect world, computer security would be easy. It would make perfect sense, be predictable, foreseeable, and perfectly functional. Security practices would be taught in every basic computer literacy course as early as students begin using computers, and everyone would understand that writing down a password, and hiding it under a mouse pad is NOT a good security plan – in a perfect world.

This world is far more interesting. The business environment does not often promote sensibility or predictability, much less any “easy” solutions. Deadlines, cutbacks, profitability, and time to market are far more indicative of this business culture. Often, executives talk about Security as something they take very seriously, but at a very high level. The truth about implementing security is that the proof is in the details. Very few security solutions are “high level” solutions. System integrity and availability are ensured where the rubber meets the road.

Every implementation of security has the potential to render an application unavailable. Every user who is unable to “work” is a potential call to the help desk. There are two rules of applying security principles to a production network:

- Use a test environment. The best way to avoid making a mistake is to have already made it and resolved it.
- Make sure that management understands (to some degree) and approves what is being done. It is not always better to ask forgiveness than permission. Management should be sponsoring security enhancements.

1.2 The “Cost” of Security.

The cost of security is measured in dollars, and it is measured in hours. Software and hardware tools need to be purchased to protect company networks. Regular maintenance is needed to apply patches, monitor logs, and train administrators and users in the proper use of these tools. Furthermore, the cost of security is vigilance. An information system that is perfectly secure today may be completely insecure tomorrow. Tools are an important aid, but no tool can replace the watchful eye of a trained security administrator.

These costs are significant, but the costs of not securing a network are far greater.

1.3 Develop Different Policies for Different Types of Computers.

Secure installations are the result of the repeated application of standard tools and settings. Develop individual policies for desktops, laptops, Domain Controllers, File and Print Servers, Web Servers, and other application servers with unique requirements. Automate the application of these standards using the scripting tools included in Windows 2000 and the Windows 2000 Resource Kit.

Human interaction is prone to error. While scripting tools can save a great deal of time with well-tested scripts, poorly tested scripts can cause problems in many systems, very quickly. Scripts need to be tested, retested, and retested again. Scripts should also be locked down, allowing only read+execute rights to everyone (or authenticated users) and read+write+execute rights for administrators.

1.4 Enforce the “Least Privilege” Principle.

The Least Privilege Principle states that each user should be given the minimum amount of privileges on networked computers necessary to do their job. A user with unrestricted access to an entire network can cause catastrophic damage by spreading a simple “Trojan Horse” virus. A network that has no precautions whatsoever is a timebomb waiting to go off.

1.5 Avoid Granting Administrator Privileges.

Administrator – the venerable Holy Grail of hackers and crackers. This account, or its equivalent, is the trophy sought by malicious users to deface, degrade, and destroy systems and networks. A user who is a member of the Administrators group has the power to do all things, good and evil, and not necessarily be accountable for those actions.

New to Windows 2000 Active Directory Domains are the roles of the Enterprise Administrator, Schema Admins, and Domain Admins (with new implications) groups. This group is created in the first domain of a forest, and has some level of authority over all domains in a forest. Enterprise Administrator rights are required to add domains to the forest, and perform other Enterprise level functions.

Restrict administrative rights whenever possible. When not possible, make sure the users with these rights – and their supervisors – understand what has actually been given to them, and the power that they may wield.

1.6 Identify the Owners of Physical and Electronic Property.

Each data file has an individual or department who “owns” the information. System administrators have the responsibility to maintain the data as required by the data owners. Develop a list of all data owners for critical data and applications on your systems. Include the department name, an individual contact name, title, phone number, names of the individuals authorized to grant access to the data, and any special data requirements. Periodically confirm and update the list.

This list can be used to verify requests for access, or for contact information if problems arise.

1.7 Limit Domain Trust.

Domain trust has been significantly transformed in comparison to the Windows NT style trusts. Now, a Windows 2000 forest of domains shares a Global Catalog, Schema, and Domain Naming Context. Consolidating unsecured domains into a common forest plays right in with Microsoft’s Active Directory goals of domain consolidation, and is quite convenient. It also presents new security risks unless all domains in a forest are properly secured.

Non-transitive, one-way trusts are still available to support backward compatibility to Windows NT domains. Using these trusts may be necessary to maintain security boundaries between trusting domains. Not all domains should be trusted or consolidated. If a domain in a forest becomes compromised, the forest would effectively be compromised. Domains and forests create security boundaries, and should be used carefully.

1.8 Restrict Modems in Workstations and Servers.

With the exception of company monitored, secured, and maintained dial-in services, active modems in workstations and servers present a potential security risk, and should only be used when absolutely necessary.

Modems can allow improper access into and out of the network. Modems set to autoanswer open the system up to war-dialer attacks. Modems also allow the users to bypass the firewall or proxy servers when accessing the Internet. This can allow NetBIOS scans of the system that would normally be blocked by the firewall or router. When a modem is necessary, such as in a dial-up server, try to obtain a phone number for the line which is far outside the range of phone numbers assigned to an organization by the phone company. This will make it more difficult for war-dialers to find the modem. Also, do not publish this number, warn support staff against social engineering tricks to obtain the number, and train night watchmen to report endless calling to different phones all night long.

To check your network for active modems, consider running your own war-dialer. You can also write a script to connect to all of your systems and search for active device drivers/services that indicate the presence of a modem, e.g., modem.sys or RAS. There are also Enterprise Management Systems, such as Bindview NOSadmin or SMS Server, which can inventory hardware or search for modem device drivers and dial-up

services. Another option is to use NBTSTAT.EXE to scan your network for machines with registered NetBIOS names for the RAS service.

Phone companies or internal phone systems may give the option to enable phone lines for dial-out access only. This represents an excellent defense against war-dialer attacks.

1.9 Limit Access to “Sniffer” Software.

Windows 2000 Server products ship with an optional packet sniffer tool: Network Monitor. This tool can compromise security in those cases where non-administrative users can run it. It enables anyone using SMS (or anyone with access to the SMS installation media) on the network to capture frames to and from any Network Interface Cards (NICs) in the agent machine. Therefore, it should be password protected (using a good password) through the Monitoring Agent control panel applet to guard against rogue SMS installations.

The decision to NOT run Network Monitor or other Sniffer software on any network must be a management decision. Users who are “Administrators” of their own workstations can not be technically restricted from installing software on their workstations. Administrators must be vigilant in periodically searching for Network Monitor agents. These may be compromised, and used against a company’s own network.

Note, however, that even administrators who have explicit “No Access” to something can grant themselves access. It is important to realize that an administrator can do anything to the system and then hide his/her tracks. View who has Network Monitor installed on a domain computer by choosing the Identify Network Monitor Users option from the Tools menu. Another requirement of sniffers is that they use a network adapter that operates in “Promiscuous Mode” – it is capable of listening to all local network traffic, not just traffic it is intended to receive.

Other sniffer programs are available on the Internet – in the form of freeware, shareware, and commercial programs, and most have functional trial downloads. These programs must be discouraged as a matter of policy.

Using switched networks as opposed to shared networks can mitigate some of the effectiveness of sniffer software, but can still be subject to attack. Shared networks use a network connection as if it were a party line – everyone can talk, and everyone can listen – and everyone “should” listen and respond only to the information intended for them. Switched networks establish direct connections, as opposed to party lines, for more efficient communication.

Limit Network Monitor access to only those users who need to use it. Very few administrators actually need to use sniffer tools.

1.10 Keep Systems Software Up To Date.

Microsoft continuously releases updates to the operating system in the form of Service Packs and Hotfixes. Service Packs are larger updates, which address numerous issues and used to contain feature upgrades (although Microsoft has ceased its practice of including new functionality in Service Packs since Windows NT 4.0; Service Pack 4.) Hotfixes are released between Service Packs to address a single issue. It is important to keep up to date with both Service Packs and Hotfixes, as they often patch important security holes. However, it is just as important to test both in your environment before applying them to production systems. Both Service Packs and Hotfixes have created new security and operating problems in the past. Generally speaking, a Hotfix which has been fully regression tested and is fully supported should not cause any problems. However, you should still always test both service packs and Hotfixes on a non-production machine before applying them to production machines.

Third-party tools are available to assist administrators with the daunting task of keeping up with the latest Hotfixes and patches. Two such tools are SPQuery, available from St. Bernard Software (<http://www.stbernard.com>) and Service Pack Manager by Gravity Storm (<http://home.san.rr.com/gravitystorm>).

These tools will obtain a list of all available Hotfixes for the Service Pack on the system and then determine which Hotfixes have been installed. Often, the tools offer the ability to quickly apply the Hotfixes both locally and remotely.

One utility available from Microsoft, QFECHECK.EXE, will perform same function on the local machine.

Software updates are collections of individual program fixes, which may include in security fixes and enhancements. New Service Packs almost always offer enhanced security over earlier Service Pack levels. Microsoft is also well known for requiring the latest Service Pack on an operating system before continuing further technical support.

Windows 2000 is capable of integrated OS and Service Pack installation, as well as combined Service Pack and HotFix installation. More information is available from Microsoft at <http://www.microsoft.com/windows2000/library/planning/incremental/sp1guide.asp>

1.11 Update and Practice a Recovery Plan.

Without question, disasters will happen. Lightning will strike, and no system is immune to some form of outage, whether it be the result of malicious activity, hardware failure, software incompatibility, or human error. Every Windows system administrator will eventually be faced with a true emergency and will have to recover, rebuild, or restore a server from a state of disaster, back to production.

Rather than waiting until absolutely necessary, it is a good practice to become familiar with some of the recovery options early, make a plan, take notes, and gain an understanding of what tools are available. Ensure not only that production systems are recoverable, but also that security settings are recoverable or repeatable as well. Practice using those tools and be ready and knowledgeable when problems arise and time is critical.

1.12 Require Strong Passwords.

The most common security policy measure in use today is the use of an account for the purpose of identification, and a secret password used as authentication. Stronger, more complex passwords significantly add to the security of a network. Human nature dictates that users will use passwords that are easy to remember, and will leave reminders of these passwords in the event that they are forgotten.

Implementing strong, complex passwords will have an effect on every user. While this is very important, it is likely to increase the number of support calls by users with password problems. Enforcing this policy should be a management decision, with full management support when users complain about these policies. It is also important to emphasize that Services running under User (or Administrative) Accounts should have complex passwords, and those should be changed on a regular basis.

Because of the method used in storing the LanMan password hashes, passwords could possibly be guessed if they are greater than 7 characters, but less than 14 characters long. Passwords which are not easy to guess (random characters, for example) can not be guessed in this manner. More information on cracking password hashes is available at <http://www.sans.org/infosecFAQ/win/logon.htm>.

Encourage strong passwords through education of techniques such as mnemonics, keyboard patterns, and shifting for touch-typists.

1.13 Require Password Protected Screen Savers.

Users should be trained to lock their workstations when they are not in use. In the event that they forget to lock their console, management should dictate a policy that users engage a screen saver (of the users' choice) after 15 minutes of inactivity, and that it be password protected.

Servers and Administrators' workstations should be implemented the same way, but should activate after only 5 minutes of inactivity due to the capabilities of Administrator rights. Another option for these machines is to use the WinExit Screen Saver which will log users off after a specified period of time.

1.14 Establish Auditing and Review Policies.

Management should be aware of how Windows machines audit security related events, and what sort of information can be retrieved as needed. Give Management the option of deciding what should or should not be audited. They may decide that is a technical decision, or they may want to set standards at their level. In any case, document policies on what should be audited, and implement that policy. Sensitive systems' audit logs should periodically exported to a secure repository, and archived to secure, physical media.

1.15 Require Administrators to Maintain a User and an Administrator Account.

The fact that a person has administrative rights over a system does not mean that they have to be using those rights to perform each and every task they do, even though it may seem like it.

Management should require that administrators maintain two accounts: An administrative account for the tasks that require elevated privileges, and a normal user account for all other functions. Windows 2000 has a new tool to facilitate switching between security contexts: RUNAS.EXE. Some tools enable "RUNAS" as an option when launching programs from the "Start Menu" by right-clicking individual programs. Some programs may require holding down the <SHIFT> key and right-clicking the programs.

1.16 Create an Administrator Password Control Process.

Every system administrator knows that each member or stand-alone server or workstation, regardless of which operating system is running on it, has local accounts – at least an Administrator and a Guest account. Strong security practices dictate that these passwords are retained in case of emergency, and would also dictate that they are all different to avoid passthrough authentication between nodes in case one of the passwords is compromised.

Establish a password management policy – one which can not be easily guessed, or inferred. Provide a place to physically lock them up, and keep them available in the event of an emergency. Local Administrator account passwords need to be maintained for Windows 2000 machines to make use of the Recovery Console, which will be discussed later in this document. If machines are cloned, local passwords should be changed prior to final deployment.

1.17 Require Virus Protection Software.

The most common threat from the Internet today is the threat of malicious program code. Most often, that threat can be mitigated or eliminated by using and maintaining virus protection software. Dozens of brand names are available, and some are free for personal use. This inexpensive investment provides the most basic protection against malicious code of many types.

Policy should dictate that an Antivirus program is installed on every networked computer, and that it should never be disabled. It should update virus definition files from vendors on a weekly basis (several times a week for critical systems) and the virus "engine" should be updated as necessary.

The Melissa virus proved two things: First, that people will generally open any E-Mail sent to them, and second, that E-Mail viruses spread following daylight – they can spread as fast as the earth turns. Most E-Mail servers have the ability to integrate Antivirus packages and detect known viruses before they ever get to the user. Some "SPAM" filters may help as well.

1.18 Recommend Host Based Intrusion Detection Systems (IDS).

Antivirus utilities have gone above and beyond protection from viruses, and provide basic defense against many back-door programs that could otherwise ravage a network.

Antivirus programs can not, however, see an attack coming. Intrusion Detection Systems come in two basic types: Host Based and Network Based. Network Based IDS can be a firewall, packet filter, or other network device. A Host Based IDS runs on each machine and monitors all traffic in and out, in order to watch for malicious code or commands.

Also part of this category are System State monitors. These are similar to Host Based IDS, as they run on the local machine. They watch critical files – like registry keys, or web site pages – for unauthorized changes, and set off alarms of many sorts if necessary. Tripwire is a popular System State monitor.

In any case, companies should consider Host Based IDS for critical systems to mitigate the effects of system security failure.

Incident Response goes hand-in-hand with IDS. If there is no Incident Response Plan, an Intrusion Detection System has little value. More information is available at http://www.sans.org/y2k/sec_policy.htm#6.4.

1.19 Perform Periodic Low-Level Security Audits.

This text reports many of the known security problems with Windows security, and solutions to those problems. At some point in time, in any size environment, some detail will be overlooked. The best way to find those loose details is to periodically audit these supposedly secure networks. Auditing can be done internally on the systems themselves, or externally from the network, or a combination of both.

Scans should include checking for open and active ports on development, lab, and production systems. Additionally, run L0phtcrack against password databases on stand-alone servers and one Domain Controller from each domain.

Audits should be scheduled at least quarterly for all critical systems, and on each new system as it is brought onto the network. In addition, it would be best to schedule audits after any changes are made, or after new vulnerabilities are discovered.

Be wary of unscheduled external/3rd party audits – they might look very much like an actual attack on the network. Make sure they are scheduled and approved before Security Vulnerability Assessment or Penetration Testing ever begins. Make sure everyone is aware of what is happening, and has at least an approximate timeframe of the test.

Some vulnerability checking utilities check for Denial of Service attacks by actually launching those attacks. Such testing should be done in non-production time if possible.

1.20 Be Quick to Disable Accounts of Terminated Employees.

In the event that an employee must be terminated, that employee's account should be disabled immediately. If that employee was an administrator, all remote access and user accounts that employee had access to should have their passwords changed immediately as well.

The disabled user ID should be retained for a period of time, in order to determine that no access requires that specific ID. After sufficient time has elapsed, and it has been determined the ID can be deleted safely, do so. This should all be a matter of policy.

1.21 Establish and Practice System and Application Recovery Plans.

Never work without a safety net. In the event that something goes wrong, whether as the result of an attack or user error, data must be recoverable. Windows 2000 has some new features that can aid in system

recovery if properly enabled. Those same tools can help recover applications running on a given server, but some applications require additional steps to ensure the integrity of recovered data.

Some backup/recovery utilities have difficulty backing up files which are current in use by other processes on a system. Files like the registry, event logs, database files, etc. do not backup cleanly without help. More options are discussed in chapter 7.

The most important factor in system and application recovery is to establish recovery requirements, test backups and restores against those requirements, and revise the procedures necessary for each type of application server. Learn this lesson before disaster strikes in order to reduce downtime when systems fail.

© SANS Institute 2001, All Rights Reserved

CHAPTER 2 PHYSICAL DATA SECURITY

Few rules of security can be stated as simply as this:

**IF YOUR COMPUTERS ARE PHYSICALLY COMPROMISED, STOLEN, OR DESTROYED,
IT IS VERY DIFFICULT TO PROTECT YOUR DATA OR ENSURE ITS AVAILABILITY!**

Physical security of your information technology is something often taken for granted. Steps should be taken to ensure that physical assets are protected from tampering, theft, fire, flood, and power outage. All copies of the information stored on those machines should be treated with the same level of protection.

2.1 Enable the End User to Protect Laptops.

During 2000, more than 387,000 laptops were stolen. The replacement cost alone was more than \$775 million, but the cost of proprietary information that was compromised will never be known. Although no piece of property is worth risking life and limb, some steps can be taken to protect laptop computers.

- Don't write passwords down. If they must be written down, don't leave them in the laptop case.
- Don't carry laptops in standard "this is a laptop" type cases. If a carry-on bag says "Dell" or "Compaq" on it, everyone knows it's a laptop. Choose something more like a briefcase, and put something bright and identifiable on it. That hot-pink luggage tag might make for an interesting conversation piece at meetings, but it will also be visible from across the room in an airport.
- Be especially careful at airport x-ray machines. Don't put laptop bags on the conveyor belt until AFTER the person in front of you has cleared the metal detector. A common ploy is for a team of two people to get in front of someone with a laptop. The first goes through without any problem. The second holds up the line, (usually with keys and change in every pocket,) while the laptop has already gone through, and been stolen by the first.
- Give all travelers security cables and teach them how to use them.
- Encourage the use of the Encrypting File System (discussed later in this chapter) to add another layer of protection for critical data.

2.2 Physically Secure Servers.

Protect servers' consoles from unauthorized access:

- Place the server in a locked room with access controlled by the administrator.
- Re-key all locks upon moving in and whenever keys are found to be out of control.
- Number all keys and track individually.
- Verify that drop-down ceilings and raised floors do not allow uncontrolled access.
- (Advanced) Provide electronic access control and recording for the server room and review access list on a regular basis not to exceed every 6 months.
- Lock the CPU case and set up a procedure to ensure the key is protected and yet easily available to the administrator. Make a back-up key and protect it off-site in a secure disaster recovery site or a safety deposit box or similarly protected place. Also lock the server down with a cable or in a rack. If physical protection is adequate and case or rack locks are not allowed, consider using frangible evidence seals to reveal tampering
- (Advanced) Use surveillance cameras to record who accesses the equipment.
- Arrange the room so that the keyboard is hidden from view by prying eyes at windows or other vantage points.

2.3 Protect the Server from Unattended Reboot.

Windows NT was notoriously vulnerable if a malicious user were to gain physical access to a machine. Windows 2000 is only slightly more secure under those same conditions, and only if the Encrypting File System

is utilized. The following steps may seem like common sense, but are recommended to maintain basic physical protection from unauthorized rebooting if physical access is compromised:

- Ensure that the computer first boots from the hard drive, then from the floppy and/or CD-ROM. This “boot sequence” is configured in the system’s BIOS, which is typically accessed by hitting a special key (such as DEL or Ctrl-S) during early boot up. Watch for an on-screen message and refer to the owner’s manual to discover this key sequence and to learn how to modify BIOS settings.
- On mission-critical servers, disable the floppy drive and CD-ROM in the BIOS. There is a registry setting to disable these under Windows NT; however, this setting only disables them as network shares. They are still available to the local user and can still be used to boot the computer. For even better security, remove them from the computer case. Step 3.4 discusses the registry key.
- If the machine is not in a physically secure room, set a BIOS password to prevent the boot sequence and other parts of the BIOS from being changed.
- Windows 2000 integrates power features to allow some machines a graceful shutdown by pressing the power button, even without being able to log on. Not all computers will support these power options, but they may be able to be configured in the “Power” Control Panel applet.

Caveat: Setting the BIOS password can disable automatic restart. If you need to allow the server to restart automatically after a power outage or other problem, don’t set the BIOS password. On servers that allow it (IBM servers are one example) set “network node” in the BIOS so that the computer can restart but the keyboard is locked until the BIOS password is entered. In addition, most BIOS manufacturers provide a “back-door” into their BIOS, significantly compromising security. Therefore, relying simply on BIOS passwords is by no means sufficient.

2.3.1 Protect the SAM with SYSKEY.

What? Windows 2000 already protects the SAM with SYSKEY – right? Well, it does, but there’s still an old Linux utility (available at <http://home.eunet.no/~pnordahl/ntpasswd>) that can beat both NTFS file systems, and SYSKEY protection. It can be used to disable SYSKEY, and rewrites the Administrator password hash with a different one.

If the computer is compromised, this utility will crack it, in spite of all that SYSKEY can do. SYSKEY should be used, with either a password (best for laptops,) or with a diskette (which could be left in servers,) in order to protect encryption keys used by the Encrypting File System, discussed later in this chapter. Type “SYSKEY” at the command prompt and click Update for more information.

2.4 Protect the Backup Tapes.

Although greatly improved from Windows NT, the built-in Windows 2000 backup tool (NTBACKUP.EXE) does not encrypt tapes, it only encrypts those files designated by the Encrypting File System (EFS). Third-party backup software may do so, but often does not by default. Files that are protected on the file system can be compromised if back-up tapes can be analyzed. Most backup software has an option to restrict access to the tapes to administrators, which is a good first step to protecting tapes.

- Put the backup tape drive in a secured room.
- Set up a secure off-site storage system for back-up tapes.
- For short-term storage, place backup tapes in a locked cabinet and establish a procedure for controlling access to the tapes. Note: In general, the built-in backup tool does not provide sufficient functionality for production servers.
- Ensure that the tape rotation scheme is sufficient to protect the system and meet any legal requirements.
- Many records (employment records, payroll data, etc.) are subject to federal, state, or organizational retention requirements. These backups should comply with these requirements. For example, if

payroll data must be maintained for seven years, ensure that backup tapes are not overwritten after one year. Many organizations make a special backup for long-term retention. Media in long-term storage should be maintained on a regular schedule and periodically tested for media or data degradation. Use the list of data owners to periodically verify the adequacy of file retention. Also keep any special hardware or software necessary to restore this data.

- In the case of special long-term backups, it may be acceptable to write the data directly to CD media, which may be retained indefinitely.

Common Tape Rotation Schemes								
Scheme	Daily		Weekly		Monthly		Archival Backups	
	Back-up Method	Retention Schedule	Back-up Method	Retention Schedule	Back-up Method	Retention Schedule	Back-up Method	Retention Schedule
Grandfather -Father-Son	Incremental or Differential	2 Weeks	Full	4 – 5 Weeks	Full	One Year	Full	As Required
Father-Son	Incremental or Differential	2 Weeks	Full	5 – 6 Weeks	N/A	N/A	Full	As Required

2.5 Use NTFS Disk Partitions.

NTFS provides advanced security features superior to FAT file systems, including the ability to apply specific file and folder permissions, ownership, auditing, encryption and compression. Other features exist which are not available on FAT partitions. Note that many of these features may be combined, with one exception: encryption and compression may not be used together.

Early adopters of Windows NT were hesitant to use the NT File System because they were familiar with the FAT file system. DOS enabled access to all files, without restriction, and NTFS was viewed as an obstacle to data recovery in the event of a system failure. Even long after NT was widely accepted, NTFS still presented problems due to the lack of a boot-time command line interface and “Safe Mode” as was available with the Windows 9x operating systems. This functionality was only available in conjunction with third-part utilities such as NTFS-DOS.

Windows 2000 offers significant improvements over Windows NT with regard to native NTFS disk access. Now, boot time options include a Safe Mode, a Safe Mode with Command Prompt, and a Recovery Console. Together, they offer a great many options for booting inoperable systems, and are discussed in greater detail in Chapter 5.

With those fears out of the way, Windows 2000 attempts to install to NTFS partitions by default. All fixed disks should be formatted with NTFS partitions.

2.6 Enable the Encrypting File System.

Windows 2000 supports transparent file-level and folder-level encryption. On an NTFS Volume, right-click the desired file or folder, and select Properties. On the properties page, click Advanced to bring up the advanced properties. Check the “Encrypt contents to secure data” checkbox, and click OK. If a file is being encrypted, the next window will ask if the file, or the parent folder and its contents are to be encrypted. If a folder is to be encrypted, the next window will ask if that folder, or that folder and its contents are to be encrypted.

Windows 2000 encrypts files with a randomly chosen File Encryption Key. This key is then encrypted with the user’s Public Key for safekeeping. In the event that the encrypted files need to be decrypted by a system administrator in an organization, that File Encryption Key is also encrypted with the Public Key of the Recovery Agent. Computers that are members of an Active Directory domain have the domain Administrator account as the default Recovery Agent. Other computers have the local Administrator as the Recovery Agent.

Be wary of the fact that EFS will temporarily place an unencrypted copy of files in the %systemdrive%\temp folder, which can be undeleted. Also be sure not to encrypt an entire hard drive – it will likely leave a system entirely unusable.

Here are a few other important notes on using the EFS:

- Install the High-Encryption Pack (available from Microsoft TechNet at <http://www.microsoft.com/TechNet/win2000/w2kencrm.asp>)
- Maintain the latest service pack on the computer.
- Use SYSKEY and either store the system key on a diskette, or derive it from a passphrase.
- Run KEYMIGRT.EXE to upgrade the protection of private keys (See Microsoft bulletin at <http://www.microsoft.com/technet/security/bulletin/ms00-032.asp>)
- Enforce a strict password policy. When it comes down to it, encryption keys are ultimately protected by account passwords.
- Periodically test file recovery. Always test file recovery after changing Recovery Agents.

2.6.1 Using the Encrypting File System on Portable Computers.

One noteworthy problem exists with regards to the Encrypting File System on computers that are not physically secured. A computer can be rebooted with a specific diskette, which provides access to the Administrator account with a blank password. (Available at <http://home.eunet.no/~pnordahl/ntpasswd>) If the Recovery Agent is the local Administrator – or any other local user – it can be compromised by this utility.

The only ways to protect against this attack are to either use a domain account as a Recovery Agent, choose another SYSKEY protection option (see “Protect the SAM with SYSKEY” earlier this chapter,) or to use a third party encryption utility that is not bound to user accounts.

2.6.2 Backup the File Encryption Certificate and the associated Private Key.

When using the File Encryption System (EFS), it is possible for the private key to become corrupt. Since the File Encryption Key (FEK) is encrypted with the private key, such corruption would make all encrypted files and their backups unrecoverable.

In order to backup the FEK, follow these instructions:

- log in as the local File Recovery Agent – usually the Local Administrator.
- Click Start, and click Run. Type MMC.EXE and click OK.
- On the Console drop-down menu, click Add/Remove Snap-In.
- Click Add.
- Click Certificates, and click Add. Choose “My User Account” and click Finish.
- Then click Close, and click OK.
- In the left pane, expand Certificates, and Personal, and select the new Certificates folder.
- Double-click Administrator in the right pane.
- Select the Details tab, and click the “Copy to File” button.
- This will start the Certificate Export Wizard. Click Next to begin the export process.
- Select “Yes, export the private key” and click Next.
- If the key is to be removed from the computer, ensure that the “Delete the Private Key if export is successful” option is checked. Click Next.
- Type and confirm a unique password to secure the exported key. Click Next.
- Choose a filename for the exported key. Click Next.
- Click Finish and close all open windows.

Save the key to diskette, and LOCK IT UP! Lock up the password, preferably in a separate location, and DO NOT store them with the computer.

2.6.3 Recovery Agent Management.

Managing Recovery Agents for stand-alone machines, or computers in a Windows NT Domain are fairly simple. The local machine Administrator is the recovery agent. In an Active Directory domain, management gets more complicated as the domain gets larger.

In a large domain, at least two recovery agents should be defined, and they should not be Domain Administrator accounts. The first should be implemented throughout the enterprise, or forest, and should be protected by all measures possible – it is the safety net in case all other measures fail. The second should be specific to an Organizational Unit or domain, and available for regular use as necessary.

The Recovery Agent's key should never be transferred to a computer to decrypt a file – always transfer the encrypted file to a secure computer where the recovery key can be used, then return the unencrypted file to the user. Only leave the key on that computer temporarily, and maintain the physical security of the Recovery Agent key in a locked location.

2.7 Uninterruptible Power Supplies.

Power fluctuations are common, and can result in interrupted service and/or damaged hardware. An Uninterruptible Power Supply (UPS) is the least expensive insurance policy available, and should be required on all servers.

- Install a UPS and associated software that allows the server to shut down automatically and safely when the power in the UPS is about to be exhausted.
- In the case of a full-sized data center, companies should consider a large backup generator in addition to backup power supplies.

2.8 Environmental Protection.

Disaster can strike from various environmental factors, resulting in total destruction of systems and/or entire facilities. Forces of nature can destroy the best-laid plans.

- Provide temperature and humidity controls sufficient to avoid damage to the equipment. One UPS vendor provides an optional attachment that monitors temperature and humidity and can send administrative alerts and emails and can page the system administrator.
- Choose a site for a data center that affords protection from flood damage.
- (Advanced) Provide one or more chemical-based automatic fire extinguishers.
- Disaster Recovery Plans should include contracting an alternate site from disaster recovery companies. This may possibly be done in conjunction with off-site backup tape storage.
- If the business case supports it, companies should consider maintaining redundant data centers in separate geographic locations.

2.9 Windows File Protection.

A new feature of Windows 2000 is Windows File Protection. This allows a safe copy of critical operating system files to be kept in a secure location. If a file is deleted or overwritten, Windows File Protection automatically copies a known-good copy back to the original location.

In order to effectively delete these files, their "safe copy" must first be deleted. These files are located at %SystemRoot%\System32\DIICache by default. Once files are deleted from this location, they can be permanently deleted from their normal location under the %SystemRoot% folder tree.

More information on Windows File Protection is available in the Microsoft TechNet article [Q222193](#), and its configuration tool (System File Checker – SFC.EXE) in TechNet article [Q222471](#).

CHAPTER 3 WINDOWS 2000 SECURITY POLICY CONFIGURATION

A majority of the security settings that apply to Windows NT 4.0 also apply to Windows 2000. Many of the out-of-the-box vulnerabilities of Windows NT have been inherited by Windows 2000. Microsoft, as if by tradition, has favored “backwards compatibility” and “ease of use” over security in its default configuration. That is not to say that Windows 2000 is just as much of a hacker’s dream as its predecessor – there are clear enhancements that are significantly improved over Windows NT.

Many of the security configuration options of Windows NT were made by directly editing the registry. Windows 2000 replaces many of these manual registry “hacks” with policy based security settings, which can be set by the Local Security Policy tools, or assigned by Group Policy.

In order to support stand-alone workstation and server computers, as well as domain controllers and member servers, this chapter will focus on Local Security Policy. Many of these settings apply to Active Directory Group Policy as well.

3.1 Configure the Local Security Policy.

The first thing most people notice when diving into Windows 2000 is that the “Administrative Tools” are not located under the “Programs” listing like they were in Windows NT. There is an option to show them in their familiar location through Taskbar Properties/Advanced Properties, but they have been moved to the Control Panel by default.

These settings will be configured through the Local Security Policy tool in the Administrative Tools. The Local Security Policy tool is actually a snap-in executed by the Microsoft Management Console (MMC) which presents a common interface through which most tools in Windows 2000 run.

3.1.1 Configure the Account Policy.

The Account Policy is made up of the Password Policy and the Account Lockout Policy. These ultimately should be configured in accordance with individual company policies, but recommended minimum settings are as follows.

Options under the Password policy should be set to remember 8-13 passwords, with a minimum password age of 1-5 days, a maximum password age of 45-90 days, and a minimum password length of 8 characters.

Windows 2000 now offers the built-in features of password complexity, and storing passwords with a reversible encryption algorithm. Password complexity should be enabled, requiring three of the four groups of characters to be used in all passwords (uppercase alphabetic, lowercase alphabetic, numeric, and special characters).

One noteworthy point about password complexity is that, although the same functionality was available in Windows NT, it was possible to circumvent it for administrators who had access to change passwords with the User Manager for Domains. In Windows 2000 there is only one tool available to change passwords, and this password complexity rule is enforced on Administrators as well.

Another less desirable feature of Windows 2000 is the ability to store passwords using a reversible encryption algorithm. Passwords should not be stored using a reversible encryption algorithm. It is only a matter of time until a tool is available to crack passwords stored in this way (if it is not available already) and disabling this option can mitigate this risk. Note that disabling the ability to store passwords using a reversible encryption algorithm may disable some application features, such as Digest authentication in IIS.

The Account Lockout Policy options should be set to lockout accounts for four hours after five failed logon attempts, and reset accounts after four hours.

3.1.1.1 Secure the Administrator and Guest Accounts.

Special attention should be paid to the built-in Windows accounts: Administrator, and Guest. The problem with these accounts is that they both have special properties. The Administrator account can not be disabled, but the Guest account is by default, and should remain disabled. These accounts should both be given complex passwords of at least 8 characters, which should be changed regularly. They should be renamed and given obscure names. A “honeypot” Administrator account should be created with a complex password, and disabled.

Local and/or Group Policies can manipulate these accounts, as shown later in this chapter. The Administrator account should have network lockout enabled by the PASSPROP.EXE utility as described later in this chapter.

3.1.2 Configure the Local Policies.

The recommended settings for the Local Policies are detailed below:

3.1.2.1 Enable Audit Policies.

When Windows 2000 is first installed, no auditing is enabled. The following audit policies are recommended as minimum standards:

Item	What it does (from TechNet)	Recommended
Audit account logon events	Logs both local and remote resource logons.	Success, Failure
Audit account management	Audits User accounts or Groups created, changed, or deleted. User accounts renamed, disabled, or enabled. Passwords set or changed.	Success, Failure
Audit Directory service access (For DC's)	Important for Domain Controllers. Audits access to the directory service.	Success, Failure
Audit logon events	Enables auditing of logon events.	Success, Failure
Audit object access	Enables auditing on base system objects	Success, Failure
Audit policy change	Enables auditing of any changes to user rights or audit policies.	Success, Failure
Audit privilege use		Success, Failure
Audit process tracking	Tracks program activation, handle duplication, indirect object access, and process exit.	No Auditing Required. Good to monitor Virus behavior in a Development Environment.
Audit system events	Logs shutdowns and restarts for the local workstation.	Success, Failure

There is some concern regarding auditing object (file and folder) access. Just for the record, enabling audits for object access – both success and failure – does not directly cause any object auditing. It only enables the possibility of object auditing. After it is enabled, specific objects (files, folders, registry keys, or registry entries) must have auditing enabled for specific users or groups (typically, Everyone) in order to generate any audits in the Security Event Log.

3.1.2.2 Customize User Rights.

The following recommendations should be applied to user rights. Please note that new users rights in Windows 2000 are noted by *.

User Right	Possible Problems	Domain Controller	Standalone/Member Server	Professional
Access this computer from the network	Stolen administrator accounts can be used over the network. Removing the right from the administrator accounts forces these users to have physical access to the system in order to access resources.	Domain Users (remove Administrators from this right)	Domain Users	None
Act as part of the operating system	Acting as part of the operating system overrides all other rights, permissions, or privileges.	None	None	None
Add workstations to the domain	Users with this right could add another domain controller to the network and obtain a copy of the SAM database.	Administrators	None	None
Backup files and directories	Users with no permissions for certain files or folders can make backup copies. When combined with the Restore Files and Directories right, this right can allow unauthorized users to obtain copies of critical files.	Backup Operators	Backup Operators	Backup Operators
Bypass traverse checking	Allows access to files or folders regardless of the user's permissions to the parent folder. In other words, prevents the inheritance of permissions.	Administrators, Server Operators, and Backup Operators	Administrators ("Users" seems to be required for IIS)	Administrators
Change the system time	Resetting the system time can seriously impact or destroy audit trails. System time can effectively disable Kerberos security.	Administrators	Administrators	Administrators and Power Users
Create a pagefile		Domain Admins	Administrators	Administrators
Create a token object	Allows the creation of a security access token. This right should never be given to any user.	None	None	None
Create permanent shared objects				
Debug programs	Allows the user to debug processes and threads. Users with this right could modify programs to run malicious code.	None (except in off-Internet development)	None (except in off-Internet development)	None (except in off-Internet development)

Deny access to this computer from the network *	By denying Administrators access to Domain Controllers over the network they are forced to log on locally to make administrative changes.	Administrators	None	None
Deny logon as a batch job *				
Deny logon as a service *				
Deny logon locally *				
Enable computer and user accounts to be trusted for delegation *				
Force shutdown from a remote system				
Generate security audits				
Increase quotas				
Increase scheduling priority	This allows a user to increase the priority of a process. Setting a process's priority too high, can consume system resources creating a denial of service attack.	Administrators	Administrators	Administrators
Load and unload device drivers	Granting this right to a user could allow a Trojan Horse device driver to be loaded.	Administrators	Administrators	Administrators
Lock pages in memory	A user could use this right to launch a denial of service attack.	None	None	None
Log on as a batch job				
Log on as a service	The user could log on as a service with full control of the system. Some accounts, such as virus scanners, require this right and should be closely monitored.	Replicators	None	None
Log on locally	Known security bugs (such as GetAdmin) can escalate users permissions if run from the local console.	Administrators Server Operators and Backup Operators	Administrators Server Operators and Backup Operators	Administrators and Authenticated Users
Manage auditing and security log	Allows viewing and clearing of the audit logs. An attacker could clear the security log to erase evidence of the attack.	Administrators	Administrators	Administrators

Modify firmware environment values	Environment variables can be modified to point to malicious programs.	Administrators, Server Operators, and Backup Operators	Administrators	Administrators
Profile single process				
Profile system performance				
Remove computer from docking station *				
Replace a process level token	A user with this right could replace a security access token of a process with a different token.	None	None	None
Restore files and directories	Users with this right can restore files regardless of their permissions. If a user has both the Backup and Restore rights, the user could backup a malicious file from one location and use it to overwrite critical system files or to plant a backdoor. In high security environments, the Backup and Restore rights should not be given to the same users. In many systems, however, this is not a viable solution.	Backup Operators, or create a custom "Restore Operators" group.	Backup Operators, or create a custom "Restore Operators" group.	Backup Operators, or create a custom "Restore Operators" group.
Shut down the system	Users could bring the system down in the middle of critical jobs or while users are accessing system resources.	Administrators and Server Operators	Administrators	Authenticated Users
Synchronize directory service data *	Not used in the initial release of Windows 2000			
Take ownership of files or other objects	A user that can take ownership of files or objects can then modify the permissions to give him/herself full access.	Administrators	Administrators	Administrators

In blocks specifying "None" be sure that no users hold that privilege. Those blocks should be left undefined in the Local Security Policy definitions, and should be periodically audited to ensure that no users get that privilege without common knowledge.

3.1.2.3 Customize Security Options.

In the past, many of the security settings for Windows operating systems were performed by manually editing the registry of the computers to be secured. Microsoft has graciously taken many of those settings and incorporated them into this GUI tool for easy integration.

3.1.2.3.1 Additional Restrictions for Anonymous Connections.

The default choice for this setting is “None. Rely on default permissions.” The other choices are “No Access Without Explicit Anonymous Permissions,” and “Do Not Allow Enumeration of SAM Accounts and Shares.” For more information on the Null User and its place in Windows NT and Windows 2000, see <http://www.securityfocus.com/frames/?focus=ms&content=/focus/ms/nt/restrict.html>.

Select “No Access Without Explicit Permissions.”

3.1.2.3.2 Allow Server Operators to Schedule Tasks (Domain Controllers Only).

This setting should be disabled, allowing only Administrators to schedule tasks on Domain Controllers. Enabling this option would allow a Server Operator to elevate his privilege by running scheduled tasks in the System context.

3.1.2.3.3 Allow System to be Shut Down Without Having to Log On.

By default, this is enabled on Windows 2000 Professional, and disabled on Windows 2000 Server and Domain Controllers. What it does is enable or disable the “Shutdown” button on the “CTRL+ALT+DEL to login” menu.

In some rare circumstances, it may be preferable to enable this option on servers, so that data center personnel may restart systems without having logon rights. This should only be an option in environments that have a VERY high priority on physical security. In either case, this setting should be made deliberately, and should be well-documented.

3.1.2.3.4 Allowed to Eject Removable NTFS Media.

In the event that removable NTFS media is being used, care should be taken on designating exactly who may remove that media. By default, only Administrators have this right.

3.1.2.3.5 Amount of Idle Time Required Before Disconnecting Session.

Configure this setting to 15 minutes. This setting may need to be considerably longer when used with Terminal Services application servers, and individual testing should be the determining factor.

3.1.2.3.6 Audit the Access of Global System Objects.

Audit the use of base kernel objects such as mutexes and semaphores – generally only useful to developers. Leave this setting undefined or disabled.

3.1.2.3.7 Audit Use of Backup and Restore Privilege.

If an unauthorized user can restore files to a new directory, those files can be compromised. Audit all such actions. Treat users with the “Backup Files and Directories” user right as if they have read access to all of the information stored on a machine. They do, so audit their use of those privileges.

Be aware that this can generate extremely large log files – with an event written for each file backed up.

3.1.2.3.8 Automatically Log Off Users When Logon Time Expires (Local).

Any organization that makes use of the account logon times, should be logging those users off as their time expires.

3.1.2.3.9 Clear Virtual Memory Pagefile When System Shuts Down.

The Pagefile holds the contents of Virtual Memory when it is not currently in use. That being said, it is likely that somewhere in this pagefile, which usually is as large or larger than physical memory, usernames and passwords are stored on disk. If a computer were to be restarted in an alternate operating system, and the pagefile were read from disk sector-by-sector, those passwords could be discovered.

Enable this setting to clear the pagefile on shutdown to avoid this risk. Be advised that enabling this setting will cause the system to take longer to shut down. Systems with very large paging files may take a LOT longer to shut down.

3.1.2.3.10 Digitally Sign Client Communication (Always/When Possible).

At a minimum, digitally signing client communication should be enabled "When Possible." Digitally signing client communication "Always" should be used only if supported by an organizational policy. It will also break interoperability with clients not capable of SMB signing.

Be aware that Digitally signing Client communication creates a performance penalty of about 10%.

3.1.2.3.11 Digitally Sign Server Communication (Always/When Possible).

As with client communication, server communication should be enabled When Possible. Digitally signing server communication "Always" should be used if supported by an organizational policy. It incurs the same interoperability and performance implications as Digitally Signing Client Communication.

3.1.2.3.12 Disable CTRL+ALT+DEL Requirement for Logon.

The CTRL+ALT+DEL requirement for Logon should NOT be disabled – leave this option as either enabled or not configured.

3.1.2.3.13 Do Not Display Last User Name in Logon Screen.

Another subjective setting is whether or not to display the username of the last person logged on to the console. By default this setting is disabled – once again favoring ease-of-use. In situations where physical access to a server could be compromised, enable this setting to remove the name of the last user who successfully logged on to the console.

3.1.2.3.14 LAN Manager Authentication Level.

One of the strongest features of Windows 2000 Security is Kerberos authentication. Why then is there any concern over the level of LAN Manager Authentication being used? The answer is that in the event that a downlevel client (or server, for that matter) is either authenticating, or being authenticated, LAN Manager Authentication is used, opening the same vulnerabilities inherent in Windows NT.

Another potential concern is that LAN Manager Authentication is attempted after Kerberos authentication fails. If a Domain Controller were somehow disabled from performing Kerberos authentication, LAN Manager Authentication would follow.

The possible responses are as follows:

0. Send LM & NTLM Responses
1. Send LM & NTLM – Use NTLMv2 session security if negotiated (default)
2. Send NTLM response only
3. Send NTLMv2 response only
4. Send NTLMv2 response only\Refuse LM
5. Send NTLMv2 response only\Refuse LM & NTLM

If at all possible, NTLMv2 should be used across all levels of a network. This setting should be set to at least 2. Be sure to test applications thoroughly prior to widespread NTLMv2 implementation. DSCClient.exe is included on the Windows 2000 Server CD to add NTLMv2 compatibility to Windows 9x systems.

3.1.2.3.15 Message Text/Title for users attempting to Logon.

These two settings (text & title) collectively put a message of the administrators' choice on the computer console prior to logon. According to officials of the U.S. Department of Justice, legal actions against intruders have failed because the owner of the computer failed to put up the equivalent of a "No Trespassing" sign. In addition, some users complain about being monitored without having given permission to be monitored. The

logon message provides an opportunity to tell users who don't want to be monitored to stop using the system. It also can serve as a recurring reminder to users that business systems are business, and not personal systems.

A logon message should read something like this: "WARNING USE OF THIS PRIVATE COMPUTER SYSTEM IS YOUR CONSENT TO BEING MONITORED AND RECORDED. UNAUTHORIZED USE IS PROHIBITED. WE RESERVE THE RIGHT TO SEEK ALL REMEDIES FOR UNAUTHORIZED USE. EVIDENCE OF SUSPECTED ILLEGAL USE MAY BE GIVEN TO LAW ENFORCEMENT." In any case, consult proper legal counsel to establish acceptable wording of banners to be used for legal purposes.

3.1.2.3.16 Number of Previous Logons to Cache (If Domain Controller is Not Available).

In the event that a Domain Controller is unreachable, Windows NT and Windows 2000 "remember" the logon credentials of the last 10 (by default) users who logged on to that system from a domain. On servers this option should be set to zero, since cached logon credentials pose a potential authentication weakness. On desktop computers, the same setting may also be a good policy to follow.

The major exception to this rule is that it should be set greater than zero on Laptop computers. If Laptops did not retain logon information, users would not be able to log on, using domain accounts, while disconnected from the network.

3.1.2.3.17 Prevent System Maintenance of Computer Account Password.

This setting should not be defined on stand-alone machines. On workstations and servers who are members of a domain, this setting should be disabled. Allow the machine to negotiate computer account maintenance with its domain controller unless the workstation is negotiating this password directly through the Internet.

3.1.2.3.18 Prevent Users From Installing Print Drivers.

Enable this setting to restrict users from installing Printer Drivers, which run in privileged Kernel Mode.

3.1.2.3.19 Prompt User to Change Password Before Expiration.

By default, Windows will prompt users to change their passwords 14 days prior to its expiration. An organization may decide to change this setting, based on internal policy.

3.1.2.3.20 Recovery Console: Allow Automatic Administrative Logon.

One of the Windows 95/98 options that Windows NT clearly lacked was a command-line "safe mode" environment. With the advent of NTFS (referenced in Appendix A) a third-party application that allows "DOS like" access to an NTFS Partition, Microsoft was clearly lacking a command-line recovery tool.

The recovery console can be installed from the same source files which installed the operating system (Professional, Server, or Advanced Server) using the /cmdcons parameter. The Recovery Console is covered in more detail in Chapter 7.

By default, there is one major catch to the Recovery Console: The user needs to remember the password to the LOCAL Administrator account. If this account's password (which should not be used regularly, right?) can't be remembered, then the Recovery Console is unusable.

UNLESS! That is, unless this option is enabled. Most system recovery settings are not enabled until they are absolutely necessary. This needs to be enabled before disaster strikes if it is to be used. This will bypass the password prompt completely if the system is booted into the Recovery Console.

Note: Enabling this setting creates a potential security risk if the machine becomes physically compromised. In almost all circumstances, this setting should be disabled.

This setting should be disabled in almost all circumstances. If the physical security of the computer is beyond reproach, it may be reasonable to enable this option, with the full understanding that doing so is a mitigated risk.

3.1.2.3.21 Recovery Console: Allow Floppy Copy and Access to All Drives and Folders.

Another “feature” of the Recovery Console is that it does not allow indiscriminate access to the entire system by default. It allows access to the root of each drive (drives may not necessarily use the same letters they are assigned in the GUI Windows 2000) and most areas under the WINNT folder. It also only allows files to be copied from the floppy to the system. It does not allow files to be copied from the hard drives to the floppy drives.

Enabling this setting nullifies these “features” and allows pretty much unrestricted access to the entire system from a command prompt.

These two Recovery Console settings should NEVER both be enabled. No matter how physically secure these servers are, they collectively would allow a system to be compromised with a simple reboot.

3.1.2.3.22 Rename the Administrator and Guest Accounts.

The two built-in accounts for Windows NT, Administrator and Guest, are still present in Windows 2000. Where these accounts should have been renamed in the past, now they can be renamed as a matter of Local Security Policy. Rename these accounts, either here in the policy, or in the Local Machine Users and Groups MMC Snap-in.

3.1.2.3.23 Restrict the CD-ROM and Floppy drive access to locally logged on user only.

CD-ROMs and floppy disks should not be left in machines for an extended period of time. Even so, those files should not be directly accessible to users logged in over the network.

Enable restrictions on both of these settings, restricting network users from these hardware devices.

3.1.2.3.24 Secure the Netlogon Channel.

This collection of settings relates to securing the communication between domain controllers. Enable the Digitally encrypt or sign secure channel data (always) setting if at all possible on a network. If this is not possible, at the very least, enable both the Digitally encrypt secure channel data (when possible) and the Digitally sign secure channel data (when possible) settings. Digitally encrypting secure channel data implies signing that data. Enabling these settings can (and probably will) break some interoperability, especially with regards to explicit Windows NT trusts.

On a native mode Windows 2000 domain, enable the Require strong (Windows 2000 or later) session key setting. This requires that the High-Encryption Pack be installed.

3.1.2.3.25 Send Unencrypted Password to Connect to Third-Party SMB Servers.

Anyone who can convince a computer to give up its credentials in clear text can use them on the rest of the network. A machine could conceivably be used to intercept credentials, just by asking for them.

This setting is disabled by default. Do not enable it unless absolutely necessary, and even then, make sure everyone knows the risks involved.

3.1.2.3.26 Shut Down System Immediately If Unable to Log Security Audits.

The purpose of this setting is to prevent the Security Log from filling, and missing security audit events, resulting in a time period where system and security auditing does not log critical events that might indicate a system compromise.

This option should be enabled – with the full knowledge that doing so will enable a self-imposed Denial Of Service attack if the security log fills up and an Administrator is unable to access the console and clear the Security Log at the time it occurs.

If enabled, the Security Log should be expanded to as large as possible to prevent the system from shutting down in all but the most rare circumstances. Security logs are set to 512 KB by default – which is meager at best. On critical systems, consider dedicating a full 9 GB or 18 GB drive to the security log, and have those logs archived regularly.

3.1.2.3.27 Configure Smart Card Removal Behavior.

Yet another new security feature supported by Windows 2000 is built-in support for smart cards. If a smart card is removed, no action is taken (default.) If a company demands tighter security, workstations, laptops, and servers can be configured to lock the workstation, or force logoff if the smart card is removed.

3.1.2.3.28 Strengthen Default Permissions of Global System Objects.

This option is enabled by default. It ensures that permissions on new system objects are assigned Discretionary Access Control Lists (DACL) granting only Read access to non-Administrative users. This setting should remain enabled.

3.1.2.3.29 Configure Unsigned Driver Installation Behavior.

Drivers are installed in Kernel Mode – they are not subject to authentication by the rest of the operating system. As such, if malicious code were installed as a device driver, it would be able to usurp most (if not all) other security precautions applied to a computer.

Yet another Windows 2000 security feature requires (or at least supports) digital signatures of drivers by hardware manufacturers. Drivers which are not signed by the manufacturer should be considered suspicious, or even threatening.

The choices available for this option are “Silently Succeed,” “Warn but allow installation,” or “Do not allow installation.” Clearly, the most secure option would be to disallow any such installation. Certain circumstances may require the “Warn but allow installation” option, but these should be few and far between as more and more device drivers are written, and signed for Windows 2000.

3.1.2.3.30 Configure Unsigned Non-Driver Installation Behavior.

Windows 2000 supports a feature similar to Driver Signing, but for non-driver devices. Since this seems to be a nondescript category, it should certainly be changed to the “Warn...” or “Do not allow...” setting.

3.1.3 Configure the Public Key Policy.

By default, the only option under Public Key Policy is the “Encrypted Data Recovery Agents” option. Users can be configured to be File Recovery Agents under this setting. For more information on securing the Encrypting File System, refer to chapter 2.

As other agents show themselves, they will be included in future versions of this document.

3.1.4 Configure the IP Security Policy.

The IP Security Policy can be configured to restrict network traffic by source address, destination address, or port. Using IPSec Policies to block traffic at the NIC is no substitute for the use of a firewall, but it does add another layer of protection.

3.2 Group Policy

An extension of the Local Policy, Group Policy Objects can be assigned to groups of computers or users of an Active Directory Domain at either the Domain, Site, or Organizational Unit (OU) level. Doing so can override local settings. Even in the event that settings are changed locally, domain controllers refresh them periodically during logon sessions.

A true implementation of Group Policy in Active Directory is far beyond the scope of this document, but it is possible to “lock-down” most security aspects even to the chagrin of users who like to administer themselves against company policy.

3.3 Computer Management MMC Snap-In

When Windows 2000 first reached the seasoned NT system administrators, one of the first noteworthy changes was the lack of a program folder for “Administrative Tools” – having been moved to the Control Panel. From now on, according to Microsoft, systems management would be done using the MMC, or Microsoft Management Console. The MMC itself is just a shell – an environment to run different “Snap-In” programs. Of these, the most common is the Computer Management snap-in. This can be found as either part of the Administrative Tools, or as a right-click option under My Computer.

Not all of these settings apply to security, but some do. These sub-menus are detailed in the following paragraphs. MMC Snap-In components can be customized to specific situations. They can limit views of information as applicable to users’ needs. Note that limiting users views of system information does not effectively restrict that information - it only obscures it.

Once the Computer Management MMC Snap-In is open, right-click the Computer Management (top line, left-hand pane) and click “Connect to another computer...” Type the name of other machines on the network to perform the same functions on other computers from the same interface.

3.3.1 System Tools

Some of the common system tools have been grouped into one expandable menu.

3.3.1.1 Event Viewer.

Expanding the Event Viewer reveals the three standard event logs, Application, Security, and System. Other sources of events (e.g. – DNS) will be present if they are installed on the same system.

These logs can be opened, saved, cleared, filtered, or viewed from this interface. Their properties can be modified, according to individual security policies. The logs should be set to a size large enough to hold data generated between backup cycles – that is, if full backups occur weekly, make sure the log is large enough to hold a week’s worth of events. Once this size has been determined, select “Overwrite events older than...” at least the number of days between backups, or seven in the example above.

As part of regular monitoring and administration, the event logs should be saved daily in both “.evt” binary format, and comma delimited “.csv” format, to be scanned for anomalies.

3.3.1.2 System Information

Any information about a system, both hardware and software, may be located in the System Information tab. It would be beneficial to become familiar with information in this tab. As a short list, useful information includes Network, Environment Variables, Running Tasks, Loaded Modules, Services, Startup Programs, Internet Explorer settings, and other application settings.

In order to save the information to a text file for later reference, right-click System Information, and click either Save As System Information file to save in native format, or Save as Text file. System Information should be saved from time to time, and retained in order to provide a baseline reference for troubleshooting purposes. Be sure to protect any saved information accordingly.

3.3.1.3 Performance Logs and Alerts.

These counter logs, trace logs, and alerts replace the logging functionality of the Windows NT Performance Monitor. These user configurable monitors do not appear to have changed substantially beyond the new interface.

3.3.1.4 Shared Folders.

The Shared Folders portion of this Snap-In replaces some of the functionality of the former Server Manager, by allowing access to Shares, Sessions, and Open Files. Shares can be created, deleted, or modified. Thankfully, the Create Shared Folder wizard does give the option (although, not the default option) of sharing a folder with full access to Administrators, and Read access to other users. This should be the default choice of security.

3.3.1.5 Local Users and Groups

The Local Users and Groups portion of the Computer Management Snap-In works very much as would be expected, with a few twists:

- In order to set a password, right-click the user, and choose Set Password.
- The all-too-common practice of copying the Administrator account in User Manager is no longer an option. Users must be created, and then added to the Administrators group as a separate action.

With these few exceptions, practices relating to the Administrator and Guest built-in accounts should not change significantly.

3.3.2 Services and Applications

One disturbing revelation upon initial review of the Control Panel is that there is no Services applet. The Services Control Panel Applet has been moved here, along with other service-specific functions.

3.3.2.1 WMI Control

Windows Management Instrumentation, first introduced around the time of NT 4.0 Service Pack 4, takes many of the API related functions of Windows management, and applies many of them to a single interface, which is portable from the local system to others across the network.

Although this interface is largely unused, it is accessible by the Windows Scripting Host via VBScript or Jscript, and has a great deal of capability across the operating system.

Many of the details of this service are yet to be widely used, but its power and versatility, combined with its native execution by the operating system make it an ideal candidate for Trojan Horse-like exploits. If there is no utilization of this service on a network it may be advisable to disable this service.

3.3.2.2 Services.

The Services applet in the MMC gives status, and allows manipulation of services running on the current or remote machine. These can be manipulated even more so than Windows NT, with control over Startup Type, Logon Credentials, Recovery Options, and Service Dependencies. The new option – Recovery Options – permits different actions to be taken on the first, second, and subsequent failures of a service.

3.3.2.3 Indexing Service.

The Indexing Service, which was integral to IIS, is now available to the entire operating system. By drilling down into the options within the Indexing Service, individual folders can be included in or excluded from being indexed. It would be beneficial to check this, to know if a web site index was also indexing the local hard drive. Like anything else, just because it is available doesn't mean it is necessary. If the Indexing Service is not going to be used, disable it.

3.3.2.4 SNMP Service.

The Simple Network Management Protocol (SNMP) Service is not installed by default. It can be installed as an optional networking component. If it is installed, it needs to be secured. Default SNMP security is based on a Community Name ("Public" by default) and an associated level of access ("NONE", "NOTIFY", "READ ONLY", "READ WRITE", or "READ CREATE"). The Community Name acts like a password in the case of SNMP connectivity.

In the Services MMC window, right-click SNMP Service and click Properties. Click the Security tab at the top of the windows. When configuring access, ensure that the Community Name of "Public" is completely removed. Use an obscure Community Name (not "Public", "Private", or a company name). Restart the service to take effect.

SNMP can expose internal systems to hackers, especially if the SNMP Community Name has been discovered. Do not install SNMP on Windows 2000 machines – especially Domain Controllers – unless necessary.

3.4 Additional Recommended Tools and Utilities.

Windows 2000 default configuration tools provide a great deal more protection than did its predecessor. Resources not found in the default configurations still best serve some security functions.

3.4.1 Lock out unauthorized use of the Floppy Drive.

The Windows 2000 Resource Kit includes a utility called FLOPLOCK.EXE, which runs as a service, and restricts access to the floppy drive. Floplock.exe restricts use of the floppy drive to Administrators and Power Users on Windows 2000 Professional, and to Administrators on Windows 2000 Server products.

Installation of this service can be done through the Service Installation Wizard, or at the command prompt by typing the following command: `instsrv FloppyLock "ResKitPath\floplock.exe"`

3.4.2 Enable network lockout of the Administrator account.

One special feature of the Administrator account inherited from Windows NT is that it can not be locked out due to invalid logon attempts. The purpose behind this measure is that the Administrator account needs to be available in the event that every other account on a machine is unavailable. The unfortunate side effect is that the Administrator account, aside from being all-powerful, is that there are an unlimited number of tries to get the password.

In response to this problem, Microsoft released Passprop.exe – a utility which, when executed on the local machine, enables lockout on the Administrator account for network logons only. The account still does not

lockout when logging on to the console. The command syntax is "passprop /adminlockout". It is also possible to add the "/complex" parameter to force Administrator password complexity, although Administrator account password complexity is subject to the normal password complexity policy.

Editor's note: PASSPROP.EXE is not included in the Windows 2000 Resource Kit Supplement 1 – and is not installed with the original Windows 2000 Professional/Server Resource Kits. PASSPROP.EXE is located in the NETMGMT.CAB file with the original version of the Resource Kit, and needs to be extracted manually. Hopefully the next Resource Kit Supplement will fix this omission.

3.4.3 Allow Windows 95/98/Me to use NTLMv2 in an Active Directory Domain.

Windows 2000 Server products ship with DSCLIENT.EXE, which allows downlevel Windows machines to be part of an Active Directory Domain and use NTLMv2 authentication. Once all Windows 9x machines are running DSCClient, Domain Controllers should be configured to refuse any other authentication.

3.5 Disable Unused Services under Windows 2000.

One of the immutable rules of security is that the level of security decreases as system complexity increases. An easy way to decrease the complexity of a system is to remove services, utilities, and protocols which are unnecessary. One of the risks of disabling/removing services is that removal of a critical service can cripple a system, possibly beyond the point of accessibility and repair.

As a general rule, services that will not be used in any way should be disabled or removed. Any services that are to be used should be secured. While some services have distinct requirements for their removal, the INSTSRV.EXE utility can be used to remove some services from a command prompt.

Network services such as IIS, Peer Web Services, RAS, FTP, IP Forwarding, Simple TCP/IP, SNMP, etc. pose a special threat because they are listening on TCP/UDP ports, and are unlikely to be configured securely if they are left unused. Extraneous network protocols add to the same problem.

The following services need to be running on production systems. As always, any changes should be implemented in a test environment prior to using them in production.

- DNS Client
- Event Log
- Logical Disk Manager
- Plug and Play
- Protected Storage
- Security Accounts Manager
- Optional services: IPSec Policy Agent, Network Connections Manager, Remote Procedure Call, Remote Registry Service, RunAs Service

The following services may need to be enabled on Domain Controllers.

- DNS Server
- File Replication Service
- Kerberos Key Distribution Center
- NetLogon
- NT LM Service Provider
- RPC Locator
- Windows Time
- Server and Workstation – required for most tools and resource sharing

3.5.1 Remove the OS/2 and Posix subsystems.

Unless specifically required, the OS/2 and Posix subsystems should be removed from systems directly connected to the Internet. Follow these steps to remove the OS/2 and Posix subsystems:

- Edit the registry entry HKLM\System\CurrentControlSet\Control\Session Manager\Subsystems –edit the “Optional” multistring value and remove “Os2” and “Posix”.
 - **IMPORTANT:** This multistring key must NOT be deleted, and must NOT be completely blank! If it is, the next reboot will result in a Blue Screen of Death. Make sure that there are a minimum of two (preferably four) Zero byte values remaining after the Os2 and Posix values are deleted, even if there are no other multistring values remaining. These hex values can best be viewed in REGEDIT.EXE as opposed to REGEDT32.EXE.
- Delete all registry subkeys of HKLM\Software\Microsoft\Os/2 Subsystem for NT.
- Delete the following registry key:
HKLM\System\CurrentControlSet\Control\Session Manager\Environment\OS2LibPath.
- In the HKLM\System\CurrentControlSet\Control\Session Manager\Subsystems delete all entries for OS/2 and Posix.
- Delete DOSCALLS.DLL, NETAPI.OS2, OS2.EXE, OS2SRV.EXE, and OS2SS.EXE from the %SystemRoot%\System32\DllCache folder. (When Windows File Protection prompts to restore those files from the Windows CD, click Cancel and click Yes to confirm.)
- In the %SystemRoot%\System32, delete OS2.EXE, OS2SRV.EXE, OS2SS.EXE, POSIX.EXE, PSXDLL.DLL, and PSXSS.EXE.
- Reboot, and delete all files from the %systemroot%\System32\os2 folder and its subfolders.
- Reboot the computer to make changes take effect.
- Be aware that if the System File Checker (SFC.EXE) is used with original Windows 2000 CD-ROM media, the Windows File Protection Service can inadvertently restore these files.

3.6 Secure any Remote Control Programs.

Microsoft operating systems have traditionally lacked a remote-control type of program to aid in remote administration. As a response, several remote control utilities are available including Symantec’s PC Anywhere, Microsoft’s SMS, Compaq’s Carbon Copy, to name a few.

Special attention should be given to any remote control programs which simulate console access to a machine. These may give the opportunity to gain elevated rights on a system.

3.6.1 PC Anywhere.

Symantec’s PC Anywhere has been around since the days of DOS and early days of Windows. Installation and configuration tips for a PC Anywhere installation have been documented by SANS at <http://www.sans.org/infosecFAQ/win/paranoid.htm>.

At the very least, the following suggestions should be taken into account. Enable PC Anywhere hosts to use SOME form of encryption (proprietary PC Anywhere encryption should be adequate on local networks. Enable some form of password authentication to access the host – without any challenge, any user who has installed the PC Anywhere client can reboot the host. Enable logging to the Windows Event Log – for accountability of connections, disconnections, system reboots, and file transfers. Enable the console lock (or logoff) in the case of an “End of Session” and “Abnormal End of Session” properties.

PC Anywhere users should understand that they do not necessarily have sole access to the computer they are connected to. They are “sharing” the console with the physical keyboard, mouse, and monitor.

3.6.2 Windows 2000 Terminal Services – Remote Administration.

As an answer to the lack of an integrated remote access mechanism, Microsoft has offered up a Remote Administration version of their Terminal Services on all of their server products. It is only available to Administrators by default, but may be granted to other users as per Microsoft TechNet Article Q253831.

As an additional bonus, using Remote Administration Terminal Services does not require an additional Terminal Server license – It is available as part of the Windows Server operating systems.

In order to install Terminal Services, select it in the Add/Remove Programs Control Panel Applet, Windows Components. Once installed, select Remote Administration Mode.

3.7 Windows 2000 Network Interface – Disable Microsoft Network Client.

Unless there is some application related need for the Microsoft Client, or NetBIOS, they can both be unbound from their associated network adapter, but not uninstalled as that will most definitely cause application related problems. As always, put into a test environment prior to production. Follow these steps to unbind the Microsoft Client and File/Printer Sharing:

- Click Start -> Settings -> select Network and Dial-Up Connections
- Double-click the active network adapter (the following steps must be performed for EACH adapter.
- Click the Properties button.
- Click the Networking tab.
- Ensure that only the Internet Protocol (TCP/IP) option is checked, and that the Client for Microsoft Networks and File and Printer Sharing for Microsoft Networks are disabled.

© SANS Institute 2001, All Rights Reserved.

CHAPTER 4 ADDITIONAL UTILITIES

Do not install these tools en masse on production machines directly connected to the Internet – copy only the tools which will be used to those machines. Regardless of which tools are installed, protect them with file permissions and file auditing as much as possible.

4.1 Windows 2000 Support Tools

Windows 2000 includes a set of support tools on the source CD. These tools are not installed by default, but are available. They are located in the \Support\Tools folder of the installation CD. Some of the tools are listed below.

This overview is intended to provide a basic awareness of the utilities available as additions to Windows 2000.

4.1.1 Computer Management Tools.

- Dumpchk.exe – Provides dump file validation, and some analysis.
- Kill.exe – Terminates one or more tasks or processes.
- Memsnap.exe – Produces a picture of memory usage by all processes, and writes to a log file.
- Poolmon.exe – Often used to detect memory leaks.
- Reg.exe – Manipulates the registry from a command line. Note that this tool is updated from previous versions of the same tool, and the syntax should be checked before it is used.
- Tlist.exe – Lists tasks currently running on a machine.
- W2000msgs.chm – List of Windows 2000 error and event messages in Help File format.

4.1.2 Deployment Tools.

- Apcompat.exe – Application Compatibility Tool – Allows programs to run under the context of another Windows operating system (Windows 95, Windows 98, Windows NT 4.0)
- ClonePr.dll – Clone Principal – Migrates NT 4.0 users and groups to a Windows 2000 Domain. This tool could be used to gain a copy of an entire domain.
- SIDWalker – A set of tools to aid in the management of access control policies on Windows NT and Windows 2000 domains.
 - Showacccs.exe – Analyzes part of all of a Windows NT/2000 system to get collect all Security ID (SID) information from that system. It generates a CSV file for Sidwalk.exe.
 - Sidwalk.exe – Takes a file from Showacccs.exe and translates all SID information from the old SIDs to the new SIDs as part of the domain migration.
 - Sidwalk.msc – Security Migration Editor MMC Snap-In – Provides a GUI interface to SID migration, similar to Sidwalk.exe.

4.1.3 Diagnostic Tools.

- Acldiag.exe – Reads Access Control Lists from Active Directory objects and generates a report.
- Dcdiag.exe – Domain Controller Diagnostic Utility.
- Msinfo32.exe – System Information report generator.
- Snmputilg.exe – GUI version of the SNMP Utility.

4.1.4 File and Disk Tools.

- Dskprobe.exe – Windows 2000 disk sector editor.
- Filever.exe – Utility to report on the versions of the file structure, executable, and DLL files.
- Windiff.exe – File and directory comparison utility.

4.1.5 Network Management Tools.

- Adsiedit.msc – Low level editor for Active Directory objects.
- Dnscmd.exe – Command Line tool used to manage DNS servers.
- Dsacls.exe – Command Line tool used to manage Active Directory ACL entries.
- Ldp.exe – LDAP Administration Tool.
- Ipctdom.exe – Command Line Windows 2000 Active Directory domain manager.
- Sdcheck.exe – Command Line tool to display the Security Descriptor of any object in Active Directory.
- Search.vbs – VBScript to search any LDAP structure for any piece of information.

4.1.6 Performance Tools.

- Pmon.exe – Command Line tool used to monitor process CPU and Memory utilization.
- Pviewer.exe – GUI tool similar to Pmon.exe. Also facilitates stopping processes.

4.2 Windows 2000 Resource Kit Tools

As in Windows NT, Windows 2000 introduces a myriad of essential support tools, bundled together and labeled the Resource Kit. There is a Resource Kit for Professional as well as Server installations of Windows 2000. Be sure to read the licensing for the Windows 2000 Resource Kits – Microsoft has changed their licensing practices since that which was released with Windows NT.

The Resource Kit described here is the Windows 2000 Resource Kit Supplement 1, available at the time of this printing. The tools that apply specifically to security are listed below.

4.2.1 Computer Management Tools

- Elogdmp.exe – Dumps an event log from a computer to STDOUT.
- Inuse.exe – Command Line tool to replace a file that is locked “In Use.”
- Pathman.exe – Manage the system or user path environment variable.
- Regback.exe, Regdmp.exe, Regfind.exe, Regini.exe, Regrest.exe, and Scanreg.exe – Command line registry manipulation tools.
- Setx.exe – Command line tool for manipulating user or system environment variables.
- Showpriv.exe – Display users and groups granted a particular privilege.
- Svcaccls.exe – Service ACL editor – may be used to delegate control of services.

4.2.2 Desktop Tools.

- Clear screen saver – Allow the console to keep running, but stay securely locked.
- Tweak UI – An old favorite for manipulating the User Interface.
- Winexit.scr – Windows Exit Screen Saver.

4.2.3 Diagnostics Tools.

- Auditpol.exe – Command Line Audit Policy manipulator.
- Dumpel.exe – Dump Event Log into Tab delimited file.
- Enumprop.exe – Dumps all properties for any Directory Service object.
- Guid2obj.exe – Translates a Globally Unique ID (read as SID) to its Distinguished Name.

4.2.4 File and Disk Tools.

- FileSpy.exe – Monitor local and network drive activity.
- Qgrep.exe – Grep like tool for those who are missing this utility from Unix.

4.2.5 Internet Information Services.

- Httpmon.exe – Http Monitoring Tool.
- IIS Migration Wizard.
- IIS Permissions Wizard Template Maker.
- Metaedit.exe – Metabase Editor.
- Playback.exe – Tool used to record traffic sent to a web server to be replayed against another server. This looks like it could be exploited against a machine – use it on test systems only!

4.2.6 Network Management Tools.

- Atmarp.exe and Atmlane.exe – ATM Support tools.
- Cusrmgr.exe – Command Line User and Group Manager.
- Gpotool.exe, and Gpresult.exe – Group Policy management tools.
- Ipsecpol.exe – IP Security Policy management tool.
- Kerbtray.exe – Tool to monitor Ticket information on computers running Kerberos v5.
- Ntrights.exe – Grant or revoke rights on local or remote computers.
- Permcopyp.exe – Copy share and file permissions from one share to another.
- Perms.exe – Display a user's access permissions on files or folders.
- Prnadmin.dll – Allows Printer management on local or remote computers without interactive logon.
- Rassrvmon.exe, and Rasusers.exe – Tools to monitor and audit RAS Server activity and users.
- Showacls.exe, Showgrps.exe, and Showmbrs.exe – Tools to audit file ACLs, group, and users.
- Subinacl.exe – Replace one user with another user in ACLs on files, shares, or registry permissions.
- Tsreg.exe – Terminal Services Registry Editor.
- Usrtogrp.exe – Add users to groups.
- Xcacs.exe – Set any file permissions from a command line.

4.2.7 Performance Tools.

- Drivers.exe – Display information about currently loaded device drivers.
- Perfmon4.exe – New and improved performance monitor.

4.2.8 Scripting Tools.

- Autoexnt.exe – Allows execution of an Autoexec.bat like batch file at startup.
- Wmi.pm – WMI Provider for Perl scripts.

4.2.9 Security Tools.

- Dssstore.exe – Command line tool to manage Public Key Integration.
- Efsinfo.exe – Command line tool to display information of files encrypted with the EFS.

4.2.10 Additional Microsoft and Third Party Applications.

- Cconnect.exe – Concurrent connections manager.
- Internet Scanner from Internet Security Systems – works in Loopback Mode only, without licenses.
- System Scanner from Internet Security Systems.
- Cybersafe Log Analyst – Use existing reports or create new filters to weed through Event Logs quickly.
- ActivePerl build 521 with many remote administration scripts.

4.3 Freeware, Shareware, and Commercial tools.

It is not possible to create a comprehensive list of free or inexpensive security related utilities available on the Internet. It would become outdated faster than it could be used. Below are some suggestions of the types of tools which may be helpful.

PLEASE NOTE: The SANS Institute is not endorsing the products listed here. They are listed for convenience only. This list has been compiled by the volunteers participating in its the creation. Any software should be thoroughly tested in a lab environment before being implemented in production. Additional products may be listed in future versions of this guide at the discretion of The SANS Institute.

4.3.1 Use Access Control List Auditing Tools.

Auditing Access Control Lists on files, folders, and registry keys and entries is a daunting task. Changes to these objects can be audited in the Windows Event Log, but if all accesses are audited, the logs would quickly become too large to be manageable.

One tool which can make permission auditing a little easier is DumpSec (formerly DumpACL) by SomarSoft (<http://www.somarsoft.com>) is a free utility that will analyze the tree-structures in a Windows system and generate a report format that allows administrators to easily spot security settings which seem out of place. It applies to the file system, registry, printers, shares, users, groups, policies, rights, and services. DumpSec does not appear to specifically support Windows 2000, but was written for Windows NT, and appears to run well on Windows 2000. As with any tool, it should be tested thoroughly prior to production use.

4.3.2 Audit Service Pack and HotFix Levels on Windows Machines.

In order to maintain current service pack and hotfix updates, it is necessary to know what has already been installed on production machines. Recently, Microsoft has released an update to QFECHECK.EXE (<http://www.microsoft.com/downloads/release.asp?ReleaseID=27333>) which will check the current machine for service pack and hotfix level.

4.3.3 User Manager Pro and NT Service Account Manager for Windows NT/2000.

User Manager Pro by Leiberman & Associates (<http://www.lanicu.com>) can change passwords, rename accounts, and perform a plethora of User Manager related functions on (according to the web site) 10,000 machines at once.

Also available by Leiberman & Associates is NT Service Account Manager to change those passwords which are rarely – if ever – changed.

4.3.4 Event Log Monitor from TNT Software.

Monitoring Windows networks means regularly checking (at least) three event logs and other application logs on each machine. This can lead to hours each day spent watching logs – not so different from watching paint dry, and waiting for it to drip.

Event Log Monitor from TNT Software (<http://www.tntsoftware.com>) can consolidate all event logs to a central repository in real time, to provide correlation of all events in one data source. An agent must be installed on each machine to be monitored.

4.3.5 EventAdmin from Aelita Software.

A utility similar to Event Log Monitor – EventAdmin from Aelita Software (<http://www.aelita.com>) performs very much the same function, without requiring an agent on each machine.

4.3.6 Nmap.

Nmap – or Network Mapper – is available for UNIX operating systems at <http://www.insecure.org/nmap>. It is quite useful for scanning individual machines or large networks for vulnerabilities.

4.3.7 WinDump.

A good sniffer/network analyzer, available at <http://netgroup-serv.polito.it/windump> WinDump is the Windows platform version of TCPDump.

4.3.8 PGP Encryption.

PGP Security – a division of Network Associates – offers a freeware e-mail encryption/authentication utility that easily integrates into most popular E-Mail programs. It is available for download at <http://www.pgp.com/products/freeware/default.asp>.

4.3.9 HFCheck from Microsoft.

Microsoft has provided HFCheck to scan IIS 5.0 systems to ensure they have the latest Hotfixes installed. It is available for download at <http://www.microsoft.com/downloads/release.asp?ReleaseID=24168>.

4.3.10 Health Monitor 2.1.

Microsoft has included Health Monitor 2.1 with BackOffice 2000. Health Monitor centrally collects system data such as performance counters and service status, enabling detailed status summary views of each server in an organization.

4.3.11 Atelier Web Security Port Scanner.

AWSPS is a freeware package with features including port scanning, packet capture/decoding, and more. It can be downloaded from <http://www.atelierweb.com/pscan/download.htm>.

4.3.12 Anti-Trojan.

A shareware utility which detects and removes 98 of the most common Trojans, including Back Orifice 2000, Der Spaeher 2, and SubSeven 2.1. <http://www.anti-trojan.net/home.asp?l=en&t=download>

4.3.13 L0phtCrack 3.

L0phtCrack was the first and foremost tool used to expose Microsoft password hash weaknesses. L0phtCrack 3 (LC3) is now completely compatible with Windows 2000 and Active Directory. Among its many new features is the ability to crack passwords without displaying them – in order to identify weak password users without identifying the password itself. More information is available at <http://www.securitysoftwaretech.com/lc3/>.

4.3.14 ModemSwitcher.

ABSecure's ModemSwitcher automatically disables access to/from the local network when dialing out to the Internet, and re-enables the LAN connection once the dial-up connection is dropped. The evaluation copy may be downloaded at <http://www.absecure.com/products.html>.

4.3.15 Snort.

Snort is a free Intrusion Detection System, capable of performing real-time packet analysis, packet logging, and content matching. It is available at <http://www.snort.org>.

4.4 Edit the Registry.

What do you mean edit the registry? Microsoft was supposed to learn from history and make all those obscure registry settings into options in the Local Security Policy and/or Group Policy Editors, or somewhere! These were supposed to be less obscure in the new versions of Windows. Is this really an upgraded operating system?

Yes, this is an upgrade to Windows NT. While many of the critical settings have been made policy options, still others require direct manipulation of registry settings. Here are some old favorites, and new ones as they become available.

As always, a word about editing the registry: When making changes as an administrator, it is possible to cause significant problems to an operating system. When an administrator is making changes to the registry, it is possible to literally wreak havoc beyond recovery. Be sure to follow a few simple guidelines when manipulating the registry:

- Make a backup of the registry before making changes – especially in production machines.
- When making a change for the first time, use a fairly standard configuration, and use a development environment – even if it is Windows 2000 server on a desktop or laptop computer. While Microsoft asserts that 133 or 166 MHz is the required minimum, a P90 with extra memory will work, and will blue-screen as fast as anything else.
- Try to make a few changes, then reboot to apply them, and then make some more changes. Nothing is worse than applying a hundred registry changes, then trying to figure out which one caused a problem.
- If changes are to be made to the permissions of a registry entry, use REGEDT32.exe instead of REGEDIT.EXE.
- Once registry entries have been verified, export them with REGEDIT.EXE into a .REG file, which is in text format. They can be combined with Notepad, into a single (where applicable) .REG file, and can be quickly and easily imported into a system's registry by double-clicking in explorer.

These registry changes can be implemented by the Security Configuration and Analysis tool. For more information, refer to Microsoft TechNet article Q214752.

4.4.1 Disable Autorun on CD-Rom Drives.

The Autorun feature of a CD-ROM drive presents a potential security threat by automatically running code when a CD is inserted into a machine. This code could be malicious, and should only be purposely executed by the user at the console.

```
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\CDRom
Value Name: Autorun
Type: REG_DWORD
Value: 0
```

4.4.2 Controlling Remote Registry Access.

Remote access to the registry is restricted by default to the Administrators (full access) and the Backup Operators (read only). If any changes need to be made to this access, open the following registry key in REGEDIT32.EXE and set permissions on it – those permissions will be interpreted as the permissions for remote access to the entire registry.

If an application requires null-session access to the registry – consider how important that application really is, and advise against using it. If it is a necessary evil, give the Authenticated Users group Read access to this key.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\SecurePipeServers\winreg

4.4.2.1 Exception to Remote Registry Access.

One subkey to the winreg key above, called AllowedPaths, enables registry access on an exception basis. Any paths enabled under this key will be granted access in spite of the restrictions specified on the WinReg key. The AllowedPaths key should not be present.

4.4.3 Restrict Null User access to Named Pipes.

A “named pipe” is an Inter-Process Communications (IPC) channel established between two computers over a network. Applications and services attach to pipe endpoints to communicate. The registry is remotely accessed through a named pipe, as well as other services. Unfortunately, many named pipes are accessible to anonymous, null user sessions, potentially including the pipe for the registry.

Remove the names of any named pipes that you do not want null user sessions to access. If a named pipe exists, but it is not on this list, then it is not accessible to null user sessions. Removing a named pipe from the list makes that pipe inaccessible to anonymous users. Unfortunately, knowing which pipes to remove will require testing. In Windows NT, removing WinReg (named pipe registry access) to prevent anonymous access to the registry may break certain applications. Windows 2000 does not appear to have enabled WinReg as a named pipe for anonymous users.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\LanManServer\Parameters
Value Name: NullSessionPipes
Type: REG_MULTI_SZ
Value: (list of pipe names permitted anonymous registry access)

Another value that was required in Windows NT to enforce Anonymous Named Pipe control is listed below. It may or may not be required in Windows 2000. The Hive and Key are the same as the previous setting:

Value Name: RestrictNullSessAccess
Type: REG_DWORD
Value: If this value exists and is set to 0, the NullSessionPipes value above is disregarded and null sessions are allowed to all pipes. Thus, in a secure system, RestrictNullSessAccess should either not exist or be set to 1. If this key does not exist, its value is assumed to be 1.

4.4.4 Restrict Null User access to Shares.

A registry setting exists to restrict Null User access to Shares, very much like restricting Null User access to Named Pipes.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\LanManServer\Parameters
Value Name: NullSessionShares
Type: REG_MULTI_SZ
Value: (list of share names permitted anonymous registry access)

4.4.5 Mitigate the Risk of Syn Flood Attacks.

Syn Flood Attacks capitalize on the fact that Microsoft operating systems reserve certain system resources part way through the 3-way handshake in order to speed up performance while the handshake completes. A Syn Flood never completes the handshake, and some of those resources continue to be allocated, with no completion of the handshake. Eventually, system resources run out, and the result is a Denial of Service because a system is waiting for all those connections to finish.

In order to mitigate this threat, Microsoft has designated a registry value to determine the behavior to take when handling initial Syn connections in the 3-way handshake.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: SynAttackProtect
Type: REG_DWORD
Value: 2

This value should be set to 2 whenever possible. While this value provides the best protection, it may cause connectivity problems on high-latency networks. In order to still provide moderate protection, set the value to 1.

4.4.6 Disable Router Discovery.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\[InterfaceName]
Value Name: PerformRouterDiscovery
Type: REG_DWORD
Value: 0

4.4.7 Disable IP Source Routing.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: DisableIPSourceRouting
Type: REG_DWORD
Value: 1

4.4.8 Tune the TCP/IP KeepAlive Time.

This setting is most appropriate to web servers, but may apply to other applications.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: KeepAliveTime
Type: REG_DWORD
Value: 300000

4.4.9 Disable ICMP Redirects.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: EnableICMPRedirect
Type: REG_DWORD
Value: 0

4.4.10 Disable External Name Release.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Value Name: NoNameReleaseOnDemand
Type: REG_DWORD
Value: 1

4.4.11 Disable DCOM.

Disabling DCOM should be a requirement for very high security servers, but may cause problems on some application servers. This should definitely be tested before placed into production.

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\OLE
Value Name: EnableDCOM
Type: REG_SZ
Value: N

4.4.12 Remove Administrative Shares.

CAUTION: removing Administrative Shares may disable Some Enterprise Management Systems. Any network based operations (e.g. backups) that require access to Administrative Shares will also be disabled.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\LanmanServer\Parameters
Value Name: AutoShareServer
Type: REG_DWORD
Value: 0

4.4.13 Disable 8.3 Filename Creation.

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\FileSystem
Value Name: NTFSDisable8dot3NameCreation
Type: REG_DWORD
Value: 1

CHAPTER 5 FILE, FOLDER, AND REGISTRY PERMISSIONS

The first rule of securing systems is to apply all service packs and security related Hotfixes. Setting permissions on critical files, folders, and registry entries is a close second.

In many cases, the only thing standing between local user (or null user) access to a system and local administrator access is an obscure access control entry. The following lists of permissions should be applied to a system before it is put into production, and should be verified on a regular basis.

Also included in these tables are whether or not files, folders, or registry entries should be audited. Be aware that excessive auditing, especially of system files, can significantly degrade system performance and generate very large event logs, which need to be monitored regularly.

5.1 Setting Permissions Easily.

While setting permissions is a tedious task, it is as important as physical security. In addition to enabling Local Security Policies, several tools are available to set file and registry permissions. Some popular Windows 2000 Resource Kit Tools include SHOWACLs.EXE, XCACLS.EXE, and SUBINACL.EXE

It is important to note that most folders inherit the permissions of their parent folders. The following folders do not – and should not – inherit those permissions: “C:\Documents and Settings”, “C:\Program Files”, and “C:\Winnt”.

5.2 File and Folder Permissions.

There are a few notes worth mentioning with regards to Windows file permissions. The “Full Control” permission includes all rights to a file, including changing permissions on that file. Also, the “None” permission overrides all other access. If a file is set to Administrators with Full Control, and Users with None, then the Administrators (who are also users) will have no access to the file. This can be disastrous, so use the None permission carefully. Place no permissions where “N/a” is specified. Do not use the “None” permission unless explicitly specified.

Also beware of excessive auditing. Audit the (S)uccess and (F)ailure of all access by Administrators. Audit the access of other user groups (Authenticated Users, or Everyone) as necessary. Auditing all file and registry accesses will cause the Security Event Log to fill up at an alarming rate. Test these settings in a development environment in order to develop an appropriate audit plan.

File/Folder Name	Audit	Administrators & System	Authenticated Users
C:\	S&F	Full Control	Read & Execute
C:\boot.ini	S&F	Full Control	N/a
C:\ntdetect.com	S&F	Full Control	N/a
C:\ntldr	S&F	Full Control	N/a
C:\ntbootdd.sys	S&F	Full Control	N/a
C:\autoexec.bat	S&F	Full Control	Read & Execute
C:\config.sys	S&F	Full Control	Read & Execute
C:\Program Files	S&F	Full Control	Read & Execute
%windir%	S&F	Full Control	Read & Execute
%windir%*.*	S&F	Full Control	Read & Execute
%windir%\addins*.*	S&F	Full Control	Read & Execute
%windir%\config*.*	S&F	Full Control	List
%windir%\Connection Wizard*.*	S&F	Full Control	Read & Execute
%windir%\cursors*.*	S&F	Full Control	Read & Execute

%windir%\Fonts*.*	S&F	Full Control	Read & Execute
%windir%\Help*.*	S&F	Full Control	Read & Execute
%windir%\inf*.*	S&F	Full Control	Read & Execute
%windir%\java*.*	S&F	Full Control	Read & Execute
%windir%\media*.*	S&F	Full Control	Read & Execute
%windir%\msagent	S&F	Full Control	Read & Execute
%windir%\regedit.exe	S&F	Full Control	N/a
%windir%\repair*.*	S&F	Administrators: Full Control	N/a
%windir%\security	S&F	Full Control	Read & Execute
%windir%\speech	S&F	Full Control	Read & Execute
%windir%\system*.*	S&F	Full Control	Read & Execute
%windir%\temp*.*	S&F	Full Control	Traverse, Add File, Add Subdir
%windir%\twain_32	S&F	Full Control	Read & Execute
%windir%\web	S&F	Full Control	Read & Execute
%windir%\system32	S&F	Full Control	Read & Execute
%windir%\system32*.*	S&F	Full Control	Read & Execute
%windir%\system32\cacls.exe	S&F	Full Control	N/a
%windir%\system32\CatRoot	S&F	Full Control	Read & Execute
%windir%\system32\cscript.exe	S&F	Full Control	N/a
%windir%\system32\config	S&F	Full Control	Read & Execute
%windir%\system32\comcnfg.exe	S&F	Full Control	N/a
%windir%\system32\dlcache	S&F	Full Control	N/a
%windir%\system32\drivers	S&F	Full Control	Read & Execute
%windir%\system32\ias	S&F	Full Control	Read & Execute
%windir%\system32\ineterv\Metabase.bin	S&F	Full Control	N/a
%windir%\system32\ineterv\metaback	S&F	Full Control	N/a
%windir%\system32\mui	S&F	Full Control	Read & Execute
%windir%\system32\net.exe	S&F	Full Control	N/a
%windir%\system32\net1.exe	S&F	Full Control	N/a
%windir%\system32\RAS*.*	S&F	Full Control	Read & Execute
%windir%\system32\rcp.exe	S&F	Full Control	N/a
%windir%\system32\regedt32.exe	S&F	Full Control	N/a
%windir%\system32\rexc.exe	S&F	Full Control	N/a
%windir%\system32\rsh.exe	S&F	Full Control	N/a
%windir%\system32\ShellExt	S&F	Full Control	Read & Execute
%windir%\system32\telnet.exe	S&F	Full Control	N/a
%windir%\system32\tftp.exe	S&F	Full Control	N/a
%windir%\system32\Viewer*.*	S&F	Full Control	Read & Execute
%windir%\system32\wbem	S&F	Full Control	Read & Execute
%windir%\system32\wbem\mof	S&F	Full Control	Read & Execute
%windir%\system32\wscript.exe	S&F	Full Control	N/a
%userprofile%	S&F	Full Control	Change
C:\Documents and Settings\All Users	S&F	Full Control	Read
C:\Documents and Settings\All Users\Documents	S&F	Full Control	Read & Create
C:\Documents and Settings\All Users\Application Data	S&F	Full Control	Read

5.3 Registry Key Permissions.

Run the REGEDT32.EXE program, and select each of the registry keys below, and make the changes indicated. Pay special attention to the WINREG key – although this key is empty, permissions applied to this key apply to the entire registry with regard to network based registry changes.

Hive/Key Name	Audit	Administrator & System	Authenticated Users
HKLM\Software	S&F	Full Control	Read
HKLM\Software\Classes\helpfile	S&F	Full Control	Read
HKLM\Software\Classes\.hlp	S&F	Full Control	Read
HKLM\Software\Microsoft\Command Processor	S&F	Full Control	Read
HKLM\Software\Microsoft\Cryptography	S&F	Full Control	Read
HKLM\Software\Microsoft\Driver Signing	S&F	Full Control	Read
HKLM\Software\Microsoft\EnterpriseCertificates	S&F	Full Control	Read
HKLM\Software\Microsoft\Non-DriverSigning	S&F	Full Control	Read
HKLM\Software\Microsoft\NetDDE	S&F	Full Control	Read
HKLM\Software\Microsoft\Ole	S&F	Full Control	Read
HKLM\Software\Microsoft\Rpc	S&F	Full Control	Read
HKLM\Software\Microsoft\Secure	S&F	Full Control	Read
HKLM\Software\Microsoft\SystemCertificates	S&F	Full Control	Read
HKLM\Software\Microsoft\Windows\CurrentVersion\Run	S&F	Full Control	Read
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\AEDebug	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\AsrCommands	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Classes	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Console	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\DiskQuota	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Drivers32	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Font Drivers	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\FontMapper	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\IniFileMapping	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\PerfLib	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ProfileList	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\SecEdit	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Svchost	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Time Zones	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Windows	S&F	Full Control	Read
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon	S&F	Full Control	Read
HKLM\Software\Policies	S&F	Full Control	Read
HKLM\System	S&F	Full Control	Read
HKLM\System\CurrentControlSet\Services	S&F	Full Control	Read
HKLM\System\CurrentControlSet\Control\SecurePipeServers\Winreg	S&F	N/a	Everyone= None
HKLM\System\CurrentControlSet\Control\Session Manager\Executive	S&F	Full Control	Read
HKLM\System\CurrentControlSet\Control\TimeZoneInformation	S&F	Full Control	Read
HKLM\System\CurrentControlSet\Control\WMI\Security	S&F	Full Control	None
HKLM\Hardware	S&F	Full Control	Everyone: Read

HKLM\SAM	S&F	Full Control	Everyone: Read
HKLM\Security	S&F	Full Control	N/a
Hkey_Users (HKU)	S&F	Full Control	N/a
HKU\.Default	S&F	Full Control	Read
HKU\.Default\Software\Microsoft\NetDDE	S&F	Full Control	N/a

© SANS Institute 2001, All Rights Reserved.

CHAPTER 6 WINDOWS 2000 SECURITY CONFIGURATION AND ANALYSIS TOOL

The previous chapters showed how to make security related changes to a system using the conventional tools available for day-to-day system administration. Another method for making these changes is to use the Security Configuration and Analysis Tool (formerly the Security Configuration Manager) incorporated into Windows 2000. The Security Configuration and Analysis Tool allows administrators to configure security settings, perform analysis, and make necessary changes to the systems using customizable security templates.

Security templates are configured and applied using the Microsoft Management Console (MMC.EXE) with the Security Configuration and Analysis snap-in. In order to begin using it, click **Start** -> **Run**, type MMC and press Enter. Click Console -> Add/Remove Snap-In, and click Add. Scroll down and select Security Configuration and Analysis, click Add and Close, and click OK. Right-click Security Configuration and Analysis, and click Open Database. Type a new database name, and click Open. Select a security template of choice. For the starters, select BASICSV.INF or BASICWS.INF.

6.1 Applying Standard Incremental Windows 2000 Security Templates.

Windows 2000 ships with incremental security templates to meet the needs of the different Windows roles in various environments. Microsoft was kind enough to provide security templates for each of their flavors of Windows 2000. These templates are configured for basic and secure workstations and servers, as well as a compatibility configuration for workstations, and more restrictive configurations for intranet or Internet web servers. Since these templates are incremental in nature, they should be applied in order of basic, secure, and hi-security to meet Microsoft's hi-security configuration. **The templates must be applied incrementally – simply applying the HISECxx.INF template will NOT secure a computer.**

These templates have been constructed with the understanding that they are to be used on clean-installed Windows 2000 machines using NTFS volumes. Security can not be applied when Windows 2000 is installed on a FAT or FAT32 file system.

Systems that have been upgraded from Windows NT 4.0 should first have the appropriate Basic template applied to establish the default Windows 2000 security settings – with the exception of User Rights, which should be configured manually, or by another template.

6.2 Creating Custom Policies with the Security Configuration and Analysis Tool.

The easiest way to create a custom security configuration file is to open one that makes a good starting point, and tweak it accordingly.

While these default configurations certainly improve the security of any Windows system, every rule has its exceptions. Likewise, every template must be customized to support individual application servers in a useful manner. These templates should have individual security policies added to them. Once individual security templates have been saved, they can be applied, reapplied, and transferred to other systems easily and quickly.

Right-click Security Configuration and Analysis, and click Analyze Computer. At the Error Log Path prompt, select a log file and path, and click OK. The analysis will progress, and may take a few minutes. The resulting explorer-type tree shows all entries available in the Account Policies, Local Policies, Event Logs, Restricted Groups, System Services, Registry, and File System. All of the details of these topics were discussed in Chapter 3.

When drilling down to individual collections of security settings, conflicts are displayed with a red "X". Most settings are "Not Defined." In order to define a setting, or change a set value, double-click an individual setting, check the "Define this policy in this database" checkbox, and change the database value to reflect the desired security policy. Repeat this step to customize the security policy as required.

When all the desired changes are made to the database, right-click Security Configuration and Analysis, and click Save.

6.3 Default Windows 2000 Security Templates.

Contrary to popular belief, Windows 2000 does ship with security templates. Many administrators don't apply security to systems because doing so is costly in both time and tools. These security templates should be used to apply SOME level of security above and beyond a default installation.

These templates must be applied incrementally in order to be successful. They must be applied incrementally within the configuration utility, and saved as a customized template for each machine.

It is important to remember that the default security templates are to be used as an aid. They make an excellent starting point for a freshly installed machine. However, the changing climate of Windows security requires that "secure" settings be constantly maintained and revised. Never take for granted that the canned templates will make a truly secure machine.

6.4 Performing Analysis of a computer.

Once security databases have been customized for each machine, they should be kept under the proverbial lock-and-key. If these databases were to be compromised without knowledge of the administrators, widespread weaknesses could be inadvertently distributed throughout an organization.

They should also be used for regular analysis of machines to identify configuration inconsistencies, which may indicate a compromised system, and a security breach.

With the security database loaded in the MMC Snap-In, right-click Security Configuration and Analysis, and choose Analyze Computer Now. At the appropriate prompt, give a valid path for the error log, and allow the analysis to commence.

6.5 Command-Line Configuration and Analysis.

Most administrators like to implement repeatable and scriptable administrative tools. In order to facilitate scripting solutions for the Security Configuration and Analysis Tool, Windows includes SECEDIT.EXE – a command line utility that can dump, analyze, configure, and log security configuration changes once a security template has been created. The help utility is available by opening the command prompt, and typing "SECEDIT/?". More information is available at <http://www.microsoft.com/TechNet/win2000/seconfig.asp>.

6.6 Security Template Tips.

- For computers upgraded from NT 4.0 or earlier on NTFS volumes, apply the corresponding BASIC template before applying the subsequent incremental templates. Do this with caution, and in a similar test environment before applying in production.
- Use the available resources. There are many documents available by searching TechNet, which can give real-world horror stories and lessons learned.
- Don't apply templates to production without having gone through a test environment.
- Remember that these templates are incremental. Apply the SECURE templates before applying the HISEC templates.
- Remember to save the templates. They must be saved before the settings can be exported.
- "WS" in the template names (i.e. – secureWS or hisecWS) means "Workstation" or "Server".

CHAPTER 7 WINDOWS 2000 RECOVERY OPTIONS

An essential part of any security plan is a Business Continuity Plan, to recover business operations in the event that all other security measures fail, and there is a need to start over from a known-good installation.

7.1 Windows 2000 Backups.

Windows 2000 includes NTBACKUP.EXE, a backup program that differs significantly from its predecessor in NT 4.0. When executed with no command line parameters, it launches the GUI backup/restore program. When launched with parameters, it runs as the command line backup/recovery tool.

7.1.1 Baseline System Backup.

Prior to moving a system into production, but after all production applications have been installed and configured, a baseline system backup should be performed. Any services that may lock files and make them unavailable for backup should be stopped. The backup should include all local drives, and the System State.

Similarly, periodic “off-line” backups should be performed. These special backups should be retained such that the most current, and the next most current are always available.

7.1.2 Regular System Backups.

Regular system backups are the core of any disaster recovery plan. **Ensure that ‘System State’ data is backed up regularly.** System State backups can be rather large (test systems usually register between 250MB and 300MB) and contain backup copies of the registry, boot files, and the COM+ Registration Database.

Note that backing up the System State also updates the backup of the registry stored in the %systemroot%\repair\RegBack folder. This copy of the registry will be backed up to the location designated by the NTBackup utility.

Domain Controllers (at least one per domain) should have the System State backed up at least daily – perhaps more often, in order to allow for an authoritative restore if necessary. For more Active Directory Disaster Recovery tips, visit <http://www.microsoft.com/TechNet/win2000/win2ksrv/technote/adrecov.asp>.

7.1.3 Remote System Backups.

Remote systems, including their registry and other ‘System State’ information can be backed up successfully using the NTBackup utility. To capture the System State, run a backup script on the remote system through the Task Scheduler, using a file on a local hard drive as the media. Be sure to place the log file in the same location as the backup file.

NTBackup log files are stored in the profile of the user that executes the backup. If the backup is run under the security context of the System account, the logs are stored in the profile of the Default User. Only ten logs are maintained per user profile.

7.1.4 NTBACKUP.EXE - Command Line Options.

Surprisingly well hidden, the same executable that runs as a GUI program, also runs as a Command Line executable. A full tutorial of this backup utility is beyond the scope of this text – to view them, execute NTBackup.exe /?.

7.2 Emergency Repair Disks.

The Emergency Repair Disk (ERD) no longer contains a backup copy of the registry. It contains copies of the AUTOEXEC.NT, CONFIG.NT, and SETUP.LOG files. Note that Windows 2000 ERDs contain NO security related information as Windows NT did.

ERDs can only be created from the GUI interface – they can not be created from the command line. Creating an ERD also requires that the system have a working floppy drive.

7.3 Windows 2000 Backup System Security Measures.

Secure all backups so that only the owner and the Administrator have access to the backup data. Backups created by Task Scheduler processes require System access in addition to the Administrator.

Secure the tapes or disk media used for backups. Keep in mind that if access to backup media is compromised, access to data has been compromised as well.

7.4 Safe Mode.

No longer the envy of the Windows 9x flavors of operating systems, Windows 2000 is now equipped with a Safe Mode startup, which can be helpful in diagnosing and solving problem services and applications. Safe Mode installs only the minimum set of services necessary to get the machine running. It is accessible by pressing the F8 key when prompted at system startup.

One limitation of Safe Mode is that it does not appear to give the option of logging on using a domain account, even with cached credentials. A local machine account is required to log on.

Safe mode CAN run the NTBackup GUI utility, and can restore a known-good System State Backup.

7.5 Safe Mode with Networking.

As its name implies, Safe Mode with Networking has the same sort of minimal services as Safe Mode, but allows Network logons, and network connectivity.

7.6 Safe Mode with Command Prompt.

This flavor of Safe Mode uses the GUI login utility, and supports limited GUI program functionality, but has fewer services running to support the Command Line mode. It does allow full access to the local hard drives, according to the privileges available to the logon ID. A local user account will be required for logon.

7.7 Recovery Console.

Another noteworthy addition to the suite of disaster recovery tools is the Recovery Console. It can be installed from the Windows 2000 source CD, using the /CMDCONS flag, or it can be selected when booting from that CD.

The Command console is more limited than any other form of system recovery access. It requires the local Administrator account password (not just any administrator) and has a limited subset of commands. Booting to the Recovery Console should be considered the “Last Ditch Effort” to revive a system, but it is available.

By default, only certain areas of the WINNT folder, and the root of each hard drive will be accessible by the Recovery Console. Files can not be copied from the hard drive to a floppy, only from floppy to the hard drive.

A complete list of commands available when booting to the Recovery Console are available at <http://www.microsoft.com/TechNet/win2000/recovcon.asp>

Microsoft's Whitepaper that deals with Disaster Recovery and Active Directory is available at <http://www.microsoft.com/TechNet/win2000/win2ksrv/technote/adrecov.asp>.

CHAPTER 8 WINDOWS 2000 DOMAINS: ACTIVE DIRECTORY SERVICES

Simply stated, Windows 2000 is the next evolution of the Windows NT operating system. Even the name – Windows 2000 – is just a marketing term for what was previously named Windows NT 5.0. So, how much harder is this next incarnation of an old standard, anyway?

To coin a phrase from a former instructor, “Windows 2000 isn’t like NT 5.0, it’s like NT 9.0 – It is more complex by an order of magnitude.” Those words may seem excessive unless Active Directory is part of the equation.

Any authoritative guide to securing Active Directory is well beyond the scope of this document, but it is important to get a high-level understanding of how the pieces fit together.

8.1 Domain Controllers.

Windows NT 4.0 domains are made up of a single Primary Domain Controller (PDC), and normally included at least one Backup Domain Controller (BDC). All changes to a domain were applied directly to the PDC, and the PDC replicated those changes to all of the BDCs in the domain.

Windows 2000 does away with Primary and Backup roles – mostly. Now, there are Domain Controllers (DCs). They are all able to have data available for updates, and they replicate that data between each other using a “Multi-master replication” strategy. This means that each time a user changes his password, his machine can communicate with any nearby DC, without needing to reach the Primary DC directly.

Like most things, the truth is in the details. All Domain Controllers are created equal – mostly. There are still some functions that need to have a central “headquarters” of operations. For each of those tasks, called Flexible Single Master Operations (also called an Operations Master, for FSMO pronounced “fizz-moe”) one Domain Controller is designated as the FSMO Role Owner.

- The PDC (Primary Domain Controller) Emulator – One domain controller of a domain will still look and act like a PDC with respect to Windows NT 4.0 clients, member servers, and NT 4.0 Backup Domain Controllers, if any exist.
- The RID (Relative ID) Master – Hands out unique Relative ID numbers to domain controllers as required.
- The Infrastructure Master – Maintains interdomain consistency.
- The Schema Master – Maintains the Schema changes and updates.
- The Domain Naming Master – Maintains domain uniqueness, and adds or removes domains from the forest.

8.2 Trust.

By comparison to Windows 2000 domains, Windows NT 4.0 domains were relatively flat and simple, and needed to maintain trust relationships with each other in order to share resources. They referred to each other with terms like “trusting” and “trusted”. While the NT style of trusts still exist, far more common relationships between domains will involve a “Transitive Trust”, regardless whether the domains are “parent” or “child” domains in the DNS structure. Transitive domain trusts now are “Peer” domains, as opposed to the Windows NT account or resource domains.

Regardless of which type of trust is utilized, care must be taken to minimize the number trust relationships and the number of trusting and trusted domains. Windows 2000 domains allow bigger domains, and delegation of responsibility, which allow for fewer trust relationships, and simpler intra-domain structure.

8.3 Look at the trees, but see the forest.

Domains are administrative and security boundaries, which affect policies and permissions. Domain structures should mimic support structures within an organization.

Microsoft suggests that domains follow DNS hierarchy. Collections of domains that share a DNS namespace are considered to be part of the same domain (and/or DNS) tree. For example: sans.org would share a namespace with stepbystep.sans.org and windows.sans.org to form a tree.

Multiple trees – domains that do not share a namespace, but share a transitive trust – make up a forest. All of the domains of an Active Directory forest share a Global Catalog. The Global Catalog is a database maintained on at least one Domain Controller of each domain, and holds a subset of information on each object in each domain. In the example above, sans.org is its own tree, as is Compaq.com; however they could theoretically be part of the same forest, and share a Global Catalog and Schema.

8.4 Enterprise Administrator and Schema Admins.

The first domain of an Active Directory forest has two special groups – Enterprise Administrators and Schema Admins. Members of these groups can make changes to Enterprise policies, configure Enterprise policy permissions, make changes to the Schema, and grant or deny other domains joining the forest. Enterprise and Schema Administrators groups and accounts are the new “Crown Jewels” of domain forests, even above Domain Administrators.

The “Domain Admins” group is still out there, and it is still as important as ever to protect this group.

© SANS Institute 2001, All Rights Reserved.

CHAPTER 9 WINDOWS 2000 APPLICATION SECURITY

While Windows 2000 has gone to great lengths to allow for a reasonably hardened operating system, data security is still subject to each layer protecting that data. The next most vulnerable layer of data security is the application layer. Some of the integrated applications are discussed below.

One general rule of application servers still holds true: Separate applications from the operating system, and from each other as much as possible. Served applications should NOT be installed on the same disk volume or partition as the operating system – or each other if at all possible.

For instance: If a server is being implemented as a web server, install the web server software on a partition separate from the operating system. Isolate the web components to that volume as much as possible, including Metabase backups. That same server should not be used as an FTP, E-Mail, or Database server – but if it must, dedicate a separate volume for those applications. Apply user access control lists only to the partitions and applications necessary.

9.1 Internet Information Services 5.

Microsoft stated as part of their release of Windows 2000 that they were “betting the company” on this new operating system. As an inseparable part of that bet, Internet Information Services 5.0 is present in a default installation. IIS 5, as in IIS 4, has been targeted with attacks in order to “prove” how insecure Microsoft applications are. While there are a considerable number of vulnerabilities in IIS 5, it is quite improved from its predecessor. Some sound preventative measures are listed below.

If a production server is not going to explicitly use IIS, it should be uninstalled.

Perhaps one security mantra applies to Internet Information Services more than any other application put to market by Microsoft – Keep up with the latest updates. Since IIS is installed by default, and since it is constantly being targeted for weaknesses, it is important to (say it again...) keep up with the updates.

Microsoft released a roll-up patch including all previous patches for IIS 5.0 (and IIS 4.0) dated May 15, 2001. The roll-up does not include patches to optional components of IIS (e.g. Index Server and FrontPage Extensions.) More information is available at [Microsoft Security Bulletin 01-026](#).

Here are a few IIS specific guidelines:

- If either IIS or FTP are to be installed, make sure that they each have their own logical volume separate from the Operating System.
- Never install IIS Samples folders on machines connected (even loosely) to the Internet.
- Apply the HISECWEB.INF Local (or Group) Security Policy.
- Verify user `Iuser_machinename` is not part of any privileged group.
- Verify user `Iwam_machinename` is not part of any privileged group.
- The default web site is well known, and may have some inherent vulnerabilities. Delete the default web site and create a new one.
- Disable “Parent Paths” in scripts.
- Enable Logging of SSL Events (errors and warnings) with the following registry setting:
 - Hive: HKEY_LOCAL_MACHINE
 - Key: System\CurrentControlSet\Control\SecurityProviders\SChannel
 - Value Name: EventLogging
 - Type: REG_DWORD
 - Value: 3
- Disable Indexing of the Scripts folder.
- Disable directory browsing in the Site Property sheet.
- Remove FrontPage extensions if they are not going to be used.

- Create a Certificate Trust List (CTL). Ensure the “Trusted Certificate Authorities” has been set. If a CTL has not been created, IIS will trust certificates from any Certificate Authority.
- Ensure Script Source Access is not enabled.
- Disable Internet Printing - Delete MSW3PRT.DLL.
- Secure the IIS anonymous access account.
 - Either: Uncheck the “Allow IIS to control password” checkbox and change it regularly,
Or: If an administrator can’t HONESTLY manage this password on a regular basis, leave this box checked, and allow IIS to do so.
 - The *lusr_machinename* account needs the “Log on locally” user right.
 - The *lusr_machinename* account should not have the “Access this computer from the network” user right.
- Disable use of the Command shell with #exec:
 - Hive: HKEY_LOCAL_MACHINE
 - Key: System\CurrentControlSet\Services\w3svc\Parameters
 - Value Name: SSIEnableCMDDirective
 - Type: REG_DWORD
 - Value: 0
- Remove unused script (MIME) mappings.
 - Open the Internet Services Manager.
 - Right-click <WEB SERVER> and select <PROPERTIES> <MASTER PROPERTIES> <WWW SERVICE> <EDIT> <HOMEDIRECTORY> <CONFIGURATION>
 - Remove the following and all other unused references:
 - .HTR – Web based password resets. If .HTR is required, patch according to MS00-044 (TechNet article Q267559)
 - .CMD and .BAT (Command and batch files)
 - .printer – Web based printing.
 - .IDA and .IDC (ADO is normally used instead)
 - .SHTM, .STM, and .SHTML (Server Side Includes)
 - Other suggested Script Mappings to remove if possible:
 - .CDX (Channel Definition Files)
 - .CER (Used to support certificates)
 - .IDQ and .HTW (for Index Server)
- Remove RDS Functionality – may allow shell command execution over port 80 (HTTP). (See <http://www.microsoft.com/security/bulletins/MS99-025faq.asp>)
 - If RDS functionality is not needed, remove the following folders (if installed):
 - Virtual Directory: /MSADC
 - %systemdrive%\Program Files\Common Files\System\MSADC\Samples
 - Remove the following registry keys:
 - HKLM\System\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory
 - HKLM\System\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory
 - HKLM\System\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\VBBusObj.VBBusObjCLS
- Ensure ASP Debugging is disabled in a production environment.

Attached are a few FTP Server specific notes:

- Dedicate ANY volume accessible by the FTP server explicitly to the FTP Service.

- Enable Directory Annotation
 - Hive: HKEY_LOCAL_MACHINE
 - Key: System\CurrentControlSet\Services\MSFTPSvc\Parameters
 - Value Name: AnnotateDirectories
 - Type: REG_DWORD
 - Value: 1
- Create a file named ~ftpsvc~.ckm containing the banner/warning text required by security policy.

Here are a few comments regarding the Index Service:

- As with anything else, if this is not to be used, disable or remove it.
- Edit the file %systemroot%\system32\noise.dat, and add any words which should be ignored.
- Alternate language “noise” files have extensions indicating that specific language.

Microsoft released a patch to a critical security hole on May 1, 2001. This is not the only patch that needs to be applied, but this one stands out due to its threat level. Any Windows 2000 Server system running Internet Information Services 5.0 should be patched according to the Microsoft bulletin at <http://microsoft.com/technet/security/bulletin/MS01-023.asp>.

9.2 Telnet Server.

Windows 2000 Server ships with a built-in Telnet server. By default, it is set to Manual startup, and should be disabled if it is not going to be used. One potential problem created by use of Telnet is that it is an inherently insecure protocol – it passes logon credentials in plaintext, and is subject to eavesdropping. Even if Telnet is configured to use NTLM authentication, it is still subject to automatic password sniffing. Due to these circumstances, Telnet may not be the best choice of remote administration tools, in favor of a third-party Secure Shell application.

If it is to be used for remote administration, create a local group named TelnetClients – if this group exists, Telnet will restrict its use to its members.

9.3 File and Printer Sharing.

Traditionally, File and Printer Sharing has been addressed as a part of the operating system, as opposed to its own application. In light of how IIS has been integrated into the operating system, and the number of vulnerabilities that are specific to this topic, File and Printer sharing should be regarded in its own separate application area as well.

In a move that will surely be remembered for generations to come, Microsoft has propagated the “Null User” vulnerability (null username and password) from Windows NT, and has perhaps made it worse. Typically, null user sessions are created between computers as NetBIOS/SMB (Server Message Block) connections, and are used largely to transfer data in the background, in order to support certain functions. Null Sessions are guilty of allowing considerable leakage of information concerning Windows systems.

Windows 2000 does not use Null Sessions, but supports them in the name of backward compatibility. It doesn't even need to use NetBIOS for SMB Traffic – instead using SMB/CIFS (Common Internet File System) which uses TCP/IP Port 445 instead of Ports 137/139.

Disabling Null Sessions on NetBIOS ports works the same way as it did in Windows NT. Unfortunately, there is no way (as of the time of this writing) to disable null sessions on SMB/CIFS ports, which make it vulnerable to any other Windows 2000 system, or Windows NT 4.0 (Service Pack 6a+) system.

Countering this vulnerability involves either blocking the ports at the perimeter (and other strategic points in large environments) or disabling File and Print Services. Disabling these services can be done by opening the Network and Dial-Up Connections applet in the Control Panel, clicking the Advanced tab, and clicking Advanced Settings. Then uncheck “File and Printer Sharing for Microsoft Networks” and click OK to save changes.

9.4 Microsoft Windows Services For Unix 2.0.

In order to “play well with the other children” Microsoft has introduced Services for Unix (SFU). Microsoft SFU includes a Telnet server, an NFS (Network File System) server, and an NFS client. These canned installations should be customized before being placed on a production network. In order to customize this installation, open the included “Services for UNIX Administration” MMC Snap-in.

- Configure the “Server for NFS” to map to a user server, log events, and reclaim locks after 90 seconds.
- Configure the “Client for NFS” to map to a user server.
- Configure the “Telnet server” to “Log events in the Application Log”, and log all types of events.

Note that configuring the Telnet server to use only NTLM authentication will effectively disable the use of this service to all non-Microsoft Telnet clients. Using NTLM authentication opens the system up to automatic password sniffing, while not using NTLM authentication requires sending usernames and passwords in plaintext. If neither of these options is acceptable, telnet should be entirely disabled in favor of a Secure Shell client/server.

NFS Shared folders must also be protected against unauthorized access. SFU shared folders do not have the same “hand holding a folder” icon that other shared folders have. In fact, there is no indication of what folders are shared from an Explorer window. In order to get a list of all NFS Shared folders, right-click any folder, and choose properties. Click the “NFS Sharing” tab. Click the “Share this folder” radio button, then click the “Do not share this folder” radio button, and click OK. NFS Sharing will display a list of all NFS Shared folders. Each of these folders must have its permissions reviewed.

For each shared folder, right-click that folder, and choose properties. Click the “NFS Sharing” tab. Click the Permissions button. Select the “All Machines” entry, and change the “Type of Access” to “No Access”. Proceed to add the appropriate permissions for all trusted users/machines. Repeat this process for the remaining NFS Shared folders.

9.5 Microsoft Exchange, Outlook, and Outlook Express.

Microsoft Exchange, Outlook, and Outlook Express comprise the Microsoft E-mail clients and server infrastructure. Microsoft produces updates to these products more often than administrators can realistically keep up. Updates to Outlook and Outlook Express are generally geared to protection from new script-based viruses like Melissa, Loveletter, etc. which still have variants regularly cropping up. It is extremely difficult to keep up with updates to these problems on all desktops as fast as viruses can propagate – which is something of an irony – virus writers can distribute their code faster than the major software distributors.

In order to protect E-mail servers from this malicious code, it is necessary to run E-mail based antivirus utilities, and to keep the server and antivirus software updated on at least a weekly basis. In order to be truly secure, dis-associate the .VBS extension with the CSCRIPT.EXE or WSCRIPT.EXE executable. Be aware that this will remove Visual Basic Scripting functionality from that given user or machine profile.

Unfortunately, there is no easy answer to updating software on desktops. This is where large-scale software distribution packages shine. Microsoft Systems Management Server, Tivoli, etc. all provide the capability to distribute software in a fashion capable of keeping up with latest updates.

Another option would be to use desktop E-mail packages that are not as tightly integrated to the operating system as to be vulnerable to these attacks. Programs like Eudora, Lotus Notes, and Netscape to name a few, may not natively execute VB Script or Java Script, and offer a layer of security by the simple fact that they are less compatible with some of the code used in writing modern day viruses. Of course, by giving up that integration, users would be giving up a set of features offered by the fact that Microsoft products are tightly integrated together.

9.6 Microsoft SQL Server.

Many of Microsoft's technologies that are most easily exposed are front-end systems – that is they are the workstations, web clients, E-mail clients, and programs that access data stored on back end systems. Whether those back end repositories are based on SQL Server, Oracle, or another database, security needs to be incorporated into those systems from the very beginning. How many SQL Servers are currently in production on the Internet today with system administrator accounts with the default name “sa” and the default blank password? How often do the others change their passwords? How often are those systems formally or informally audited? Are the event logs reviewed on a regular, timely basis?

While a full description on the secure implementation of database servers is far beyond the scope of this document, knowledgeable database and system administrators can and should develop a security plan to keep these systems as safe as possible.

9.7 Terminal Services Application Server.

Windows NT 4.0 offered Terminal Services as a completely different operating system. Windows 2000 offers it as well, but as a removable component in standard server operating systems. The Terminal Services shipping with Windows 2000 is actually based on Citrix' flavor of terminal services.

While having Terminal Services Application Servers in conjunction with thin clients can be an excellent strategy for server based computing, it does introduce its own flavor of security problems in the enterprise.

Here are some best practices applied to Terminal Services Application Servers:

- Do not install Terminal Services in “Compatibility Mode”. Install in the secure mode.
- When used in an Active Directory domain, take a look at Microsoft TechNet article [Q260370](#).
- Use a Domain Controller as the licensing server – if a TS Application Server needs to be rebuilt (which may happen periodically,) it won't affect licensing.

© SANS Institute 2001

APPENDIX A USEFUL WEB SITES AND MAILING LISTS

Network security is a team effort. No single person can be responsible for every aspect of network security. Below is a list of useful web sites and mailing lists which can help keep any security administrator up to speed on new bugs, vulnerabilities, attacks, and problems as they are discovered. Many of the web sites have their own mailing lists, so please check them out thoroughly.

Web Site URL:	Description:
http://www.sans.org	The SANS Institute
http://www.sans.org/giac.htm	SANS Global Incident Analysis Center
http://www.microsoft.com/security	Microsoft Security
http://www.securityfocus.com	SecurityFocus.com Press Center
http://www.windowsitsecurity.com	Windows 2000 Magazine Security Site
http://www.securityportal.com	Security Resource and Services Provider
http://www.microsoft.com/TechNet/Security/secpatch.asp	Where to find Microsoft Security Patches
http://grc.com	Gibson Research Corporation Security Software
http://www.edelweb.fr/EdelStuff/EdelPages	French Windows Security Resource
http://www.cert.org	Carnegie Mellon Internet Security Research Center
http://www.datafellows.com	Mobile, Distributed Enterprise Security Information
http://www.infosyssec.org	Extensive System Security Internet Portal
http://www.esecurityonline.com	Security Site and Newsletter
http://www.duke.edu/~tom/toolz.html	Latest Hacking Tools
http://www.whitehats.com	Security News and Tools
http://www.packetstorm.securify.com	Security Information Library
http://www.insecure.org	Home of Nmap Security Scanner

Mailing List URL:	Description:
http://www.sans.org/sansnews	Several SANS newsletters, including Windows Security Digest
http://www.counterpane.com/crypto-gram.html	Counterpane's Crypto-gram newsletter
http://infosecuritymag.industryemail.com	Security Wire Digest
http://www.ntbugtraq.com	NTBugTraq – Windows Security Bug/Exploits List

APPENDIX B WINDOWS 2000 SECURITY CHECKLIST

The next several pages are a quick checklist which can help to summarize steps taken to secure individual Windows systems. Hard copies of this checklist may also prove useful for long-term documentation of preventative measures.

Note that most of the extra utilities are not listed on this checklist. This should only be used as a "Quick Hit" list for baseline configurations. It does not represent a complete solution, and should not be taken as such. A combination of these settings, and tools listed in this entire guide should be used to create a secure Windows environment.

Steps to be taken:	Recommended:	Actual:
Protect the SAM with SYSKEY.	Password of Disk	
Protect the Backup Tapes.	Off-site storage	
Use NTFS Disk Partitions.	NTFS on all volumes	
Enable the Encrypting File System.	Enabled on Critical Folders	
Backup the File Encryption Certificate and the associated Private Key.	On diskette in a secure location.	
Uninterruptible Power Supplies.	Protecting all servers	

WINDOWS 2000 SECURITY POLICY CONFIGURATION

Configuration Setting:	Recommended:	Actual:
Configure the Account Policy.	Remember 8+ passwords. Minimum password age: 1+ Require Complex Password. Disable reversible algorithm. Enable Account Lockout to 4 hours after 5 failures and reset after 4 hours.	
Secure the Administrator and Guest Accounts.	Rename Accounts and assign 14 character complex passwords. Disable Guest.	
Configure the Local Policies.		
Enable Audit Policies.	Audit Success and Failure of all but Process Tracking.	
Customize User Rights.	Use standard user rights according to previous detail.	
Customize Security Options.		
Additional Restrictions for Anonymous Connections.	"No access without explicit anonymous permissions."	
Allow Server Operators to Schedule Tasks.	Disable	
Allow System to be Shut Down Without Having to Log On.	Disable	
Allowed to Eject Removable NTFS Media.	"Administrators" and/or specific Data Center Personnel.	
Amount of Idle Time Required Before Disconnecting Session.	15 Minutes	
Audit the Access of Global System Objects.	Disable	

Audit Use of Backup and Restore Privilege.	Enable	
Automatically Log Off Users When Logon Time Expires (Local).	Enable	
Clear Virtual Memory Pagefile When System Shuts Down.	Enable	
Digitally Sign Client Communication (Always/When Possible).	Enable "When Possible." Enable "Always" if all clients are compatible.	
Digitally Sign Server Communication (Always/When Possible).	Enable "When Possible." Enable "Always" if all clients are compatible.	
Disable CTRL+ALT+DEL Requirement for Logon.	Disable	
Do Not Display Last User Name in Logon Screen.	Enable	
LAN Manager Authentication Level.	At least 2	
Message Text/Title for users attempting to Logon.	Set these according to company legal requirements (Should be required.)	
Number of Previous Logons to Cache (If Domain Controller is Not Available).	Servers: 0 Professional: 10	
Prevent System Maintenance of Computer Account Password.	Disable	
Prevent Users From Installing Print Drivers.	Enable	
Prompt User to Change Password Before Expiration.	14 Days	
Recovery Console: Allow Automatic Administrative Logon.	Disable	
Recovery Console: Allow Floppy Copy and Access to All Drives and Folders.	Disable	
Rename the Administrator and Guest Accounts.	(Choose obscure names)	
Restrict the CD-ROM and Floppy drive access to locally logged on user only.	Enable	
Secure the Netlogon Channel.	"Digitally Sign..." and "Digitally Encrypt" when possible.	
Send Unencrypted Credentials for Third Party SMB Servers.	Disable	
Shut Down System Immediately If Unable to Log Security Audits.	Enable (be aware of consequence of enabling...)	
Configure Smart Card Removal Behavior.	Lock Workstation	
Strengthen Default Permissions of Global System Objects	Enable	
Configure Unsigned Driver Installation Behavior.	"Warn but allow installation"	
Configure Unsigned Non-Driver Installation Behavior.	"Warn but allow installation"	

COMPUTER MANAGEMENT MMC SNAP-IN.

System Tools		
Configure Event Log Settings.	Give a "large enough" size.	
Services and Applications.		
Services.		
Indexing Service.	Include public folders only.	
SNMP Service.	Disable "Public" Community Name.	

ADDITIONAL RECOMMENDED TOOLS AND UTILITIES.

Enable network lockout of the Administrator account.	Use PASSPROP.EXE from the Resource Kit	
Allow Windows 95/98/Me to use NTLMv2 in an Active Directory Domain.	DSCLIENT.EXE available from Server media.	
Remove the OS/2 and Posix Subsystems.	See section 3.5.1	
Secure any Remote Control Programs.	See section 3.6	
Windows 2000 Network Interface – Disable Microsoft Network Client.	(If not required...)	

REGISTRY CHANGES

Disable Autorun on CD-Rom Drives.		
Controlling Remote Registry Access.		
Exception to Remote Registry Access.		
Restrict Null User access to Named Pipes.		
Restrict Null User access to Shares.		
Mitigate the Risk of Syn Flood Attacks.		
Disable Router Discovery.		
Disable IP Source Routing.		
Tune the TCP/IP KeepAlive Timer.		
Disable ICMP Redirects.		
Disable External Name Release.		
Disable DCOM.		
Remove the AEDebug Key.		
Remove Administrative Shares.		
Disable 8.3 Filename Creation.		

FILE, FOLDER, AND REGISTRY PERMISSIONS – USE CHAPTER 5 AS A CHECKLIST.

APPENDIX C CHANGE HISTORY

Windows 2000 Step-by-Step v1.0 May 1, 2001

Windows 2000 Step-by-Step v1.0a May 8, 2001

- Update to process of removing OS/2 and Posix subsystems.
- Corrected typographical errors on KeepAliveTime and EnableICMPRedirect registry keys.
- Omitted change to registry key AEDebug – Do Not Delete! Protect and audit this key instead.
- Updated control of IIS anonymous account security.
- Updated usage of Telnet Server.
- Updated Mailing List entries.

Windows 2000 Step-by-Step v1.0b May 14, 2001

- Backup the System State on at least one Domain Controller at least once per day.

Windows 2000 Step-by-Step v1.0c May 20, 2001

- Implementing strong passwords should be a management decision to survive in the face of customer complaints.
- Additional update to the process of removing OS/2 and Posix subsystems.

Windows 2000 Step-by-Step v1.0d July 1, 2001

- Added short section regarding Terminal Services Application Servers.
- Updated information on available IIS 5.0 patches.

Windows 2000 Step-by-Step v1.5 July 1, 2001

- Formatted for paper printing.

© SANS Institute 2001, All Rights Reserved.