

A SURVIVAL GUIDE
FOR WINDOWS NT
SECURITY:

*A consensus document by
security professionals
from eighty-seven large
user organizations.*



WINDOWS NT SECURITY STEP BY STEP

THE SANS INSTITUTE

Version
3.03
February, 2001

THE SANS INSTITUTE

WINDOWS NT SECURITY STEP BY STEP

Version
3.03
February, 2001

A SURVIVAL GUIDE FOR
WINDOWS NT SECURITY:

*A consensus document by security professionals
from eighty-seven large user organizations.*

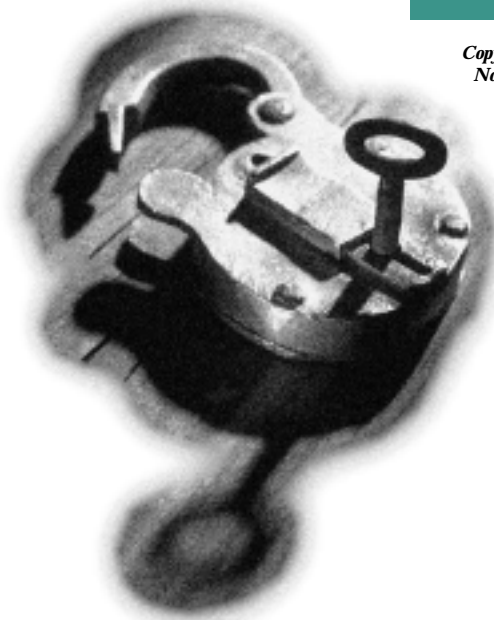
*This document is the joint product of a group of Windows NT security managers
and experts who, together, support more than 286,000 users and have more than
380 years of Windows NT security experience.*

*The SANS Institute enthusiastically applauds the work of these professionals and
their willingness to share the lessons they have learned and the techniques they use.*

Shahram Alavi, Data Security
Hilary Atkinson, Sallie Mae
Connie Balodimos, BankBoston
John C. A. Bambenek, Pentex Net
Jonathan Beyer, Andersen Consulting
Sean Boran, Boran Consulting, Ireland
David Bovée, Scitor Corporation
Kip Boyle, SRIC
Dominique Brezinski, Internet Security Systems, Inc. (ISS)
Jeffrey W. Brown, Merrill Lynch
Richard Caasi, San Diego Supercomputer Center, UCSD
Vernon A. Campbell, Telos Corporation
Harlan Carvey, Winstar Communications, Inc.
Scott Carlson, Cargill - North Star Steel

Charles Lindsay, Brooks Automation Software Corp
Thomas Linscomb, University of Texas at Austin
Chris de Longpre, Metropolitan Health Corporation
Orjan Lundberg, Luleå University of Technology, Sweden
Christopher A Lunemann, Honeywell
Rob Marchand, Array Systems Computing
Bruce K. Marshall, Feist Communications
Michael Matthews, BDM International
JD McKenna, Vitesse Semiconductor
Derek P. Milroy, MCURVE, Inc.
Rick McKinney, VISTA Computer Services
Chad Moore, US Air Force
Claude-Aime Motongane, MNCA, France

*Copyright 2001. The SANS Institute
No copying, electronic forwarding,
or posting allowed except with
prior written permission.*



Bruce Cheng, The Nature Conservancy
D. Mark Courtney, First Union National Bank
Phil Cox, CIAC
Christian Crayton, Sprint Paranet
Dennis Creagh, Taos Mountain
James M. Cullum, Metropolitan Health Corporation
MSgt Stace Cunningham, US Air Force
Marty Davidson, Oak Ridge National Laboratory
Bud Dawson, MacDonald Dettwiler, Canada
Marc DeBonis, Virginia Tech
Dennis J. Duval, Epic USA
Mark T. Edmead, MTE Software
Caryn Esten, M&I Data Services
Jim Esten, WebDynamic
Edmo Lopes Filho, Martins Com. E Servicos S/A, Brazil
Harry Flowers, The University of Memphis
Jason Fossen, Fossen Networking & Security
Lara Fulton
Paul B. Fowler, Florida Department of Revenue
Erwin Fritz and Gilbert Laustsen, Jung Associates Ltd.
Reuben Frost, Compucom Systems Inc.
Bill Genzoli, Intel Corporation
Lewis M. Getschel, Evolving Systems Inc.
Antonius J.M. Groothuizen, Eftia OSS Solutions
George Guillory, Omnitron, Inc.
David Harley, Imperial Cancer Research Fund, London
Robert J. Hensing Jr, Reynolds & Reynolds
Hobbit, Avian Research
Brantley W. Hudson, Sprint Paranet
Matti Huvila, Abo Akademi University, Finland
Daniel Isaac, Philips Research
Jesper M. Johansson, University of Minnesota
J Steven Jones, The Penrod Company
Yaron Keshet, P.S.Publishing, Israel
Jeff Klaben and Alok Kumar, NCR Corporation
Tobias Kohlenberg, Intel Corporation
Chris Lalka, Exxon Chemical Company
Joe Lawrence, Rockwell Collins
David Leblanc, Microsoft Corporation

Gregory Nash, BindView Corporation
Roger Nebel and Sammy Migues, HomeCom Communications
Michael Noonan, Intel Corporation
Stephen Northcutt, The SANS Institute
Mike O'Connor, DIBA Industries
Alan Paller, The SANS Institute
Adam Pendleton, Richard S. Carson & Assoc.
Ian Perry, Deloitte, New Zealand
A. Padgett Peterson, Lockheed-Martin Corp.
Jim Pearsall, Ranier Technology
Todd J. Pope, SAIC
James R. Skamarakas, US Army STRICOM
Gary Ragan and the Answer Desk, Collective Technologies
Gavin Reid, Cisco
Ralph A. Rodriguez, Treacy & Company, LLC
Dr. Eugene Schultz Global Integrity Corporation (an SAIC Company)
John Schumacher, Merck and Co.
Michael Sena, Denver Department of Human Resources
Paul Shields, Nortel
Gennady Shulman, John Wiley & Sons.
Peter da Silva, Bailey Network Management
Cynthia Smith, Coopers & Lybrand
Donald. J. Smith, General Dynamics
Dan Sorak, DataSystems Group
Lara M. Sosnosky, The MITRE Corporation
Calvin C. Sov, Amgen
Major Byron Thatcher, US Air Force
Jose Torres, Diageo, Plc.
Steven Tylock, Kodak, (moving to Qestra Consulting)
Carol A. Urban, Motorola Semiconductor
Eric Vandeveld, Prevea Clinic
Ian Wesley, University of Michigan
Jim White, Applied Research Associates
Curtis White, Nike
Matt Wilkinson, National Institutes of Standards and Technology
Paul G. Williams, US Air Force
Lynette Wong, State of California
Craig S Wright, DeMorgan, Australia
Kum Hon Yew, Motorola, Malaysia

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

Editors for this edition: Jason Fossen, Fossen Networking & Security
Sherri Heckendorn, The University of Texas, M. D. Anderson Cancer Center
Dave Loschiavo, Titan/Delfin
Stephen Northcutt, The SANS Institut

WINDOWS NT SECURITY

S T E P B Y S T E P

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 applies both to NT-server environments and, almost as importantly, NT-workstation environments. Since NT environments are almost universally networked, securing individual workstations is as important as securing the servers.

Windows NT 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 NT 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 NT systems and want to have confidence that they are taking steps that most experienced NT security experts take to establish and strengthen security on their NT systems.

INTRODUCTION

Though the booklet provides valuable guidance, it is not a text on the subject. Texts provide background on the way NT 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 NT 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 NT security texts, 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 NT security experts at eighty-seven large NT user organizations and a dozen smaller organizations. Together, the people who contributed substantively to this booklet have over 300 years of NT security experience and support a total NT user community of more than 252,000. The steps outlined in this booklet are the actions that they agree are important in securing Windows NT servers and workstations at their sites. Since Windows NT is 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-NT) platforms that could impact the security of the NT network should also be audited and secured.

NT Security: Step-by-Step parallels the phases of the implementation and operation of an NT system. Steps are organized into those phases and each step's description includes 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 those organizations with extremely critical security requirements, they are noted with the word "Advanced." The primary focus is on servers, connected in networks, using domain services, though some recommendations affect workstations as well.

Except as otherwise stated, all procedures in this booklet assume that one is running Windows NT 4.0 with Service Pack 3 or higher and that you have access to the Windows NT 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 having edited the registry.

Localized versions of Windows NT generally are 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 NT. Important: Updates will be issued whenever a change in these steps is required, and new versions will be published periodically. Please email ntsec@sans.org with the subject "Updates" for an immediate summary of updates and to be included in the distribution of changes as they are issued. And please tell us of any changes or additions you feel would be useful in future versions of this guide.

WINDOWS NT SECURITY

S T E P B Y S T E P

■	PHASE 0 GENERAL SECURITY GUIDELINES.....	2
■	PHASE 1 SETTING UP THE MACHINE	
■	Step 1.1 Physically secure the server.....	5
■	Step 1.2 Protect the system from undesirable booting.....	5
■	Step 1.3 Set up storage protection for back-up tapes.....	6
■	Step 1.4 Manage the Page File.....	7
■	PHASE 2 SETTING UP A SAFE FILE SYSTEM AND CREATING EMERGENCY REPAIR DISKS	
■	Step 2.1 Ensure that critical user data is stored in NTFS partitions.....	8
■	Step 2.2 Create and protect Emergency Repair Disks.....	9
■	Step 2.3 Disable POSIX and OS2 Subsystems.....	11
■	PHASE 3 SETTING REGISTRY KEYS	
■	Step 3.1 Manage logon information display and cached logons.....	12
■	Step 3.2 Use the logon message to warn away intruders.....	13
■	Step 3.3 Disable floppy disk drives and hide drive letters.....	14
■	Step 3.4 Enforce strong passwords (Registry portion).....	15
■	Step 3.5 Avoid the Netware DLL Trojan horse.....	16
■	Step 3.6 Secure print drivers.....	16
■	Step 3.7 Enable audits of backups and restores.....	17
■	Step 3.8 Restrict anonymous logon.....	17
■	Step 3.9 Control remote access to the registry.....	18
■	Step 3.10 Restrict anonymous network access to the registry and other named pipes.....	18
■	Step 3.11 Control access to the command scheduler.....	19
■	Step 3.12 Secure the Registry.....	20
■	Step 3.13 Block the 8.3 attack.....	21
■	Step 3.14 Implement NTLMv2.....	21
■	Step 3.15 Secure NetLogon Channel.....	22
■	Step 3.16 Mitigate the risk of SYN Flood attacks.....	22
■	PHASE 4 ESTABLISH STRONG PASSWORD CONTROLS AND SECURE ACCOUNT POLICIES	
■	Step 4.1 Lockout attempts to gain access after a set number and make passwords hard to guess.....	23
■	Step 4.2 Enable Administrator account lockout and rename the Administrator account.....	24
■	Step 4.3 Establish separate accounts for Administrators.....	24

CONTENTS

■ Step 4.4	Set up an Administrator password control process.	24
■ Step 4.5	Tighten the use of the Everyone Group and disable the guest account.	25
■ Step 4.6	Avoid giving Administrator privileges for most tasks	25
■ Step 4.7	Secure and Manage Event Logs.	26
■ Step 4.8	Avoid using shared accounts—along with an exception	27
■ Step 4.9	Run an ACL reporting tool	27
■ Step 4.10	Encrypt SAM's password database with 128 bit encryption	27
■ Step 4.11	Set appropriate User Rights.	27
■	PHASE 5 AUDITING	
■ Step 5.1	Turn on auditing	30
■ Step 5.2	Monitor the audit logs	31
■	PHASE 6 NETWORKING AND INTERNET SECURITY SETTINGS	
■ Step 6.1	Turn off all unneeded network services and run needed services safely	31
■ Step 6.2	If you use Internet Information Server (IIS), block known vulnerabilities.	32
■ Step 6.3	Protect vulnerable ports through a firewall (or screening router)	35
■	PHASE 7 OTHER ACTIONS REQUIRED AS THE SYSTEM IS SET UP	
■ Step 7.1	Require password-protected screen savers on all workstations	35
■ Step 7.2	Implement virus protection software	36
■ Step 7.3	Check for and remove ROLLBACK	36
■	PHASE 8 MONITORING AND UPDATING SECURITY AND RESPONDING TO INCIDENTS	
■ Step 8.1	Regularly monitor and update domain, group, user, and file security status.	37
■ Step 8.2	Establish procedures and call lists for responding to incidents	37
■	A FINAL WORD	38
■	CHECKLIST	39-49
■	APPENDIX: USEFUL RESOURCES FOR NT SECURITY PROFESSIONALS	50

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 0

GENERAL SECURITY GUIDELINES

This booklet is filled with useful actions that will help you ensure that your NT systems are properly configured and managed to reduce the risk and impact of a security incident. However, certain general security guidelines need to be followed.

STEP 0.1

Enforce the least privilege principle.

In all installations, the least privilege principle should be enforced. According to this principle, users should have only the minimal access rights required to perform their duties, e.g., only designate those users who absolutely must have administrative privileges as administrators. Also, give administrators regular user accounts and establish a policy that they should use their regular user accounts for all non-administrative duties. Administrators can use the SU utility in the resource kit to change context quickly to their administrative user account. Remember also that it is impossible to secure and perform full audits on actions by Administrators.

STEP 0.2

Carefully plan groups and their permissions.

Carefully setting up groups is the single most important thing you can do to secure an installation. NT comes with many built-in groups; several of which are useful. However, groups must match the operational model of the organization. It is, therefore, crucial to ensure that groups and access privileges are consistent with the organizational structure of your business. In addition, personnel and/or responsibility changes must be immediately reflected in the group composition and access privileges. It is also important to review the group structure periodically and ensure that it is readily understandable. A complicated group structure makes security much harder to enforce. The design of any protection mechanism should be small, simple, and straightforward.

STEP 0.3

Identify the owners of the data files on your systems.

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 system. Include the department name, an individual contact name and 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.

STEP 0.4

Limit trust.

Limit trust between domains. Trust opens a potential security vulnerability when users who should not have access to an object inadvertently are given such access. Do not use trust relationships unless necessary. With NT 4.0 trusts can be limited by the Domain Administrators within each Domain.

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 0

GENERAL SECURITY GUIDELINES

STEP 0.5

Secure RAS.

RAS is relatively insecure in a standard installation. Therefore, securing RAS is very important. Take care to grant dial-in access privileges only to those users that absolutely need them, and to revoke those privileges once they are no longer needed (see point 0.2 above). Be especially careful giving administrative accounts dial-in access. In addition, use the Microsoft Encrypted Authentication (NTLM) option and use both password and data encryption. An even better security measure would be to use third-party authentication tools for incoming RAS connections.

STEP 0.6

Do not allow modems in workstations unless 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 on a dial-up server, try to obtain a phone number for the line, which is far outside the range of phone numbers assigned to your 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 of 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 which 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.

STEP 0.7

Limit access to Network Monitor.

Windows NT Server 4.0 comes with a Network Monitor tool, a packet sniffer. This tool can compromise security in those cases where non-administrative users can run it. Limit access to Network Monitor to only those users who need to use it, probably not even all administrators. 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.

There is also a Network Monitor Agent tool that comes with both WindowsNT Server and Workstation. It enables anyone using SMS 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.

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 0

GENERAL SECURITY GUIDELINES

STEP 0.8

Use third-party authentication.

The default authentication mechanisms in Windows NT is not adequate for all security needs. In an environment where security is important, we strongly encourage you to use third-party authentication with NT, especially if you are using NT as a dial-up server. This will significantly increase your password security.

STEP 0.9

Keep your systems 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 often contain feature upgrades. 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, and Service Pack Manager by Gravity Storm. 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.

STEP 1.1.

Physically secure the server.

Problem: *Physical access to the server provides multiple opportunities to circumvent NT system access controls: the server itself or its disks could be stolen; the computer could be rebooted from a floppy disk; the operating system could be reinstalled from a CD-ROM; the information on the system could be lost through damage caused by power outages and environmental catastrophes; and passwords could be leaked by people watching Administrators work.*

- Action 1.1.1 Place the server in a locked room with access controlled by the administrator. Rekey all locks upon move in and whenever keys are found to be out of control. Number all keys and track individually. Verify that dropdown ceilings and raised floors do not allow uncontrolled access.
- ▲ Action 1.1.2 (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.
- Action 1.1.3 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.
- ▲ Action 1.1.4 (Advanced) Provide one or more chemical-based automatic fire extinguishers.
- Action 1.1.5 Install a UPS (uninterruptible power supply) and associated software that allows the server to shut down automatically and safely when the power in the UPS is about to be exhausted.
- ▲ Action 1.1.6 (Advanced) Use surveillance cameras to record who accesses the equipment.
- Action 1.1.7 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
- Action 1.1.8 Arrange the room so that the keyboard is hidden from view by prying eyes at windows or other vantage points.

PHASE 1

STEP 1.2.

Protect the system from undesirable booting.

SETTING UP THE MACHINE

Problem: *The operating system protects information under its control. If a rogue operating system is installed on the computer, information protection (other than cryptographic protection) can easily be circumvented. Rogue operating systems are most often installed from floppy disks or CD-ROM drives. Preventing users from rebooting from the floppy or CD-ROM drives may also be advisable for desktop Windows NT systems.*

- Action 1.2.1 Ensure that the computer first boots from the hard drive, then from the floppy. 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.
- Action 1.2.2 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.
- Action 1.2.3 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.

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.

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 1 SETTING UP THE MACHINE

STEP 1.3.

Set up storage protection for back-up tapes.

Problem: *The built-in NT backup tool, among its other limitations, does not encrypt tapes. 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.*

- Action 1.3.1 Put the backup tape drive in a secured room.
- Action 1.3.2 Set up a secure off-site storage system for back-up tapes.
- Action 1.3.3 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.
- Action 1.3.4 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. The backup tapes 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.

COMMON TAPE ROTATION SCHEMES								
Scheme	Daily		Weekly		Monthly		Archival Backups	
	<i>Back-up Method</i>	<i>Retention Schedule</i>	<i>Back-up Method</i>	<i>Retention Schedule</i>	<i>Back-up Method</i>	<i>Retention Schedule</i>	<i>Back-up Method</i>	<i>Retention Schedule</i>
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


PHASE 1 SETTING UP THE MACHINE

STEP 1.4.

Manage the Page File.

Problem: *The page file is used by Windows NT to move needed code and data in and out of memory when there is not enough physical RAM. Maintaining the page file on the system partition can slow system response time. When the system is shut down, data remains on disk and could possibly be read by an attacker who boots the computer with another operating system.*

- Action 1.4.1 Set page file size.
Microsoft recommends setting the page file size at the amount of RAM plus 11MB. To set the page file size, open System Properties from the Control Panel. Click on the Performance tab. The current settings are shown in the Virtual Memory section. To modify the current settings, click on the Change button. To move the page file to a partition away from the operating system, highlight the desired partition and type in the desired Initial and Maximum sizes and click the Set button. To remove the page file from the Operating System partition, set the initial and maximum sizes for this drive to zero. Note: Setting the initial and maximum sizes equal to each other will prevent the page file from growing dynamically and can improve performance.

Caveat:  Unless there is a page file on the same partition as the operating system, the system will not be able to write crashdump files in the event of a stop error.

- Action 1.4.2 Clear page file at system shutdown.

To prevent the next user from accessing the page file data written to disk, the page file can be cleared at system shutdown.

To clear the page file at system shutdown, set the following registry key:

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\Session Manager\Memory Management
Name: ClearPageFileAtShutdown
Type: REG_DWORD
Value: 1

WINDOWS NT SECURITY

S T E P B Y S T E P

STEP 2.1.

Ensure that critical user data is stored on NTFS partitions.

Problem:

Windows NT manages security only on NTFS file system partitions, and not on FAT (the traditional DOS) file systems. Originally, it was easier to recover from problems if the boot partition was FAT. However, this is no longer true. The general consensus today is that FAT should not be used on Windows NT unless absolutely necessary. For example, DEC Alpha computers require that the System Partition is FAT. Note: Systems Internals (www.sysinternals.com) sells a utility called NTFSDOS. It allows NTFS partitions to be accessed from DOS to ease recovery. However, you could also use a small NT Workstation boot partition on a SCSI ZIP disk for this purpose, or simply pull the corrupted hard drive out and put it into another case. Of course, the best option is to use a tape backup system. The main point is that there are many options when recovering a system on an NTFS partition, and therefore the use of FAT partitions is strongly discouraged. Note: Boot partition refers to the partition that holds the %systemroot% directory (often \WINNT), while system partition refers to the partition that holds the boot loader and hardware detection files (NTLDR, NTDETECT.COM, and BOOT.INI on Intel platforms).

- Action 2.1.1 Check to see if your hard drives are formatted with NTFS. In Windows NT Explorer, right-click the drive you want to check and select properties. This information window will tell you whether the disk has a FAT or NTFS file system. If your disk is NTFS, there will be a security tab for managing permissions. File system type can also be ascertained with the Disk Administrator utility, found in the Administrative Tools folder on the Start menu.
- Action 2.1.1.1 FAT volumes can be converted to NTFS without loss of data with the CONVERT.EXE utility. Convert.exe is bundled with Windows NT and very safe, but it is still a good idea to make a backup first. To convert the C: drive to NTFS, execute "convert c: /fs:ntfs" from the command line and reboot. This utility does not reformat the drive; your data will be unaffected.
- Action 2.1.2 It is very important to place users' data and operating system files into separate NTFS partitions. This will help ensure that users' files are not affected by Service Packs or upgrades, and that users do not accidentally get access to critical system files. In addition, even if users fill up their entire partition, the operating system and its paging file will be unaffected. Windows NT may crash if it runs out of available free drive space. Dedicate the C: drive to just the boot-up files (NTLDR, BOOT.INI, NTDETECT.COM, etc.) and the operating system folder (typically \WINNT).

PHASE 2

SETTING UP
A SAFE FILE
SYSTEM AND
CREATING
EMERGENCY
REPAIR DISKS

PHASE 2

SETTING UP A SAFE FILE SYSTEM AND CREATING EMERGENCY REPAIR DISKS

STEP 2.2.

Create and protect Emergency Repair Disks

Problem:

Once the operating system has been installed and the registry keys set, time will be wasted in recreating the system if there is not an Emergency Repair Disk. However, this disk can also be used by intruders since it may contain a copy of the current SAM database. An intruder will run cracking programs against the encrypted user passwords in the SAM database after stealing the disk and taking it to a safe location.

- Action 2.2.1 To create or update an Emergency Repair Disk, execute RDISK.EXE from the Run box or command line. Disks should be updated at least weekly. The program syntax is: RDISK [/s[-]] "RDISK /S" backs up the current SAM. By default, the SAM is not backed up and the first SAM from the original installation is copied to the repair disk. "RDISK /S-" will copy the repair information, including the SAM, to the %systemroot%\repair directory without user intervention or dialog boxes; it will not, however, create an Emergency Repair Disk floppy. This is useful for domain controllers where the SAM is too large to fit on a floppy. These files can then be backed up or copied to another drive. The "/S-" switch is also very useful for running scheduled registry backups. Note 1: If you run syskey to encrypt the database, you must rerun RDISK /S to ensure the backup copy of the SAM is also encrypted. Note 2: Make sure that you adequately protect the Emergency Repair Disk. It contains a copy of the SAM which can be cracked by an attacker. Note 3: Make sure that you test restores of the registry periodically to ensure that they will work properly and that you know the procedure to restore the system quickly in the event it should become necessary. Note4: The Emergency Repair process runs date-checking routines. To ensure that files are replaced correctly in the repair process you may need to replace the Setupdd.sys file on your Installation floppy disk set. If you are using Service Pack 2 or later, copy the file Setupdd.sys from the Service Pack to your Installation disk set Disk 2.
- Action 2.2.2 The Windows NT *Resource Kit* comes with a pair of utilities called REGBACK.EXE and REGREST.EXE. The *Resource Kit* can be purchased at any large bookstore. REGBACK is used to back up the registry to any directory, which can then be properly secured. REGBACK also compresses the registry. This is very useful on a DC where the SAM is too large to fit on a floppy. REGREST is used to restore the registry from that backup. You may need to be able to boot to a neutral installation to use REGREST. This can be accomplished, for example, with a minimal NT Workstation installation on a ZIP disk.
- Action 2.2.3 Set up a locked storage area for the emergency repair disks. Caveat: In large domains, recreating Emergency Repair Disks becomes less feasible and backup files are far more important.

Note: If your site has multiple DCs they can serve as the backup for each other. In this case, administrators should use rdisk without the /s option to reduce the risk of offline access to the SAM/

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 2

SETTING UP A SAFE FILE SYSTEM AND CREATING EMERGENCY REPAIR DISKS

The “registry” is a miniature database used by Windows NT to store configuration parameters for applications, hardware, security, and the operating system. The user SAM database is just one part of the registry. Registry files are stored in %SystemRoot%\System32\Config. The registry can be directly edited using REGEDIT.EXE or REGEDT32.EXE (note there is no “i” in REGEDT32.EXE).

REGEDIT.EXE is better for searching the registry and importing/exporting registry data to ASCII text files. REGEDT32.EXE must be used, however, when modifying registry values, changing permissions or managing the auditing of registry access. Both utilities can be launched from the Run box or the command line. (The Windows NT *Resource Kit* includes a number of registry-related utilities as well; on-line help with the *Resource Kit* describes them in detail.)

It is crucially important to back up any registry keys or values before modifying them. Microsoft will not support users who accidentally mangle their registries! Use REGEDIT.EXE to export a key or value to a text file before modification. To undo the change, use REGEDIT.EXE to re-import the file’s data.

Many security features are enabled by modifying the registry. If the key or value required for the security feature does not exist in the registry, it should be created with REGEDT32.EXE. Most often, you must reboot before the feature will work. Refer to the Help menu in REGEDT32.EXE for procedures.

Modifying numerous registries by hand is tedious. To automate registry modification, consider using the System Policy Editor or the Security Configuration Manager (SCM). System Policy is a technique for easily scripting registry changes and assigning these changes to individual users, groups of users, or computers. The SCM requires Service Pack 4 or later, and is a special purpose security tool that can do much more than modify the registry (see the Download section of www.microsoft.com/ntserver). The System Policy Editor is found in the Administrative Tools folder on Windows NT Server, but it must be installed on Workstation or Windows 9x.

The purpose of the System Policy Editor is to create an ASCII script based on one or more templates (such as COMMON.ADM and WINNT.ADM). No scripting skills are necessary. The script will define exactly which users, groups, and computers should receive exactly which registry changes. These changes will be automatically made when the computer reboots or the user next logs on. The script file must be named NTCONFIG.POL and saved in %SystemRoot%\System32\Repl\Import\Scripts (the folder shared as NETLOGON). The Directory Replicator Service can be used to distribute the master file to all domain controllers. See the Help menu in System Policy Editor for more information.

Many security-related registry settings are in the default policy templates. Some are not however. Fortunately, the templates can be modified by hand to include them. See the section entitled “Creating a Custom System Policy Template” in the *Windows 95 Resource Kit* for instructions.

PHASE 2

SETTING UP A SAFE FILE SYSTEM AND CREATING EMERGENCY REPAIR DISKS

STEP 2.3.

Remove POSIX and OS2 Subsystems

Problem: *These subsystems are never used, but they have privileged access to the system and could be useful to intruders.*

■ Action 2.3 Remove OS2 and POSIX subsystems:

HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\OS/2 Subsystem for NT

Remove Os2LibPath key by removing the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\Environment\Os2LibPath

Remove Posix and OS/2 keys by removing the following keys:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\SubSystems\Optional

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\SubSystems\Posix

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\SubSystems\Os2

Delete the following directory and all subdirectories.

c:\winnt\system32\os2

PHASE 3

SETTING REGISTRY KEYS

STEP 3.1.

Manage logon information display and cached logons.

Problem: *The name of a valid user could be useful to intruders who see it displayed on the logon screen. NT displays the last user name as a convenience. Also, stored passwords open huge security and auditing holes. As is often the case, you may have to trade convenience for security. Further, by default, NT stores the logon credentials for the last 10 users who logged on to the system. This is done so that the machine can be used without a domain controller, and to allow remote authentication through network boundaries. In an environment where security is important, it may be desirable to disable this behavior.*


- Action 3.1.1 Disable the display of the last logged on username by setting the following registry value. If the value does not already exist, it must be created. With REGEDT32 this is done with the Edit menu, Add Value. Enter the Name “DontDisplayLastUsername” exactly as shown and then use the String Editor to enter a “1”. Also, you can use the C2 Configuration Manager from the NT Resource kit instead of using REGEDT32.

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Name: DontDisplayLastUsername
Type: REG_SZ
Value: 1

Note: In some situations it might be preferable to allow the display of the last logged on user. E.g. certain users may not be able to remember their user name, and this would keep the administrator from having to tell them each time they logged on. Another reason you might want to display the last logged on username is because it will quickly let you know if someone else logged onto the machine. Not displaying the last logged on user name will only keep novice hackers from finding out which users exist on the machine. It is trivial for a determined hacker to get that information. Therefore, many administrators do not bother hiding the last logged on user name.

- Action 3.1.2 Disable caching of logon information by setting the following registry key. If the value does not already exist, it must be created.

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Name: CachedLogonsCount
Type: REG_SZ
Value: 0

Caveat:  *Disabling cached logons may disrupt authentication if a domain controller cannot be found. This could, for example, happen if the domain controller is on a different subnet than the client, or when users on notebook computers are away from the network. Test this in your organization before disabling cached logons.*

- Action 3.1.3 In most situations, it is undesirable to automatically log on a user. If the value AutoAdminLogon is 1 at the above location, the computer automatically logs on an administrator when the machine is started. This should be set to 0. Also, delete the DefaultPassword key, if present at this location.

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 3

SETTING
REGISTRY
KEYS

STEP 3.2.

Use the logon message to warn intruders.

Problem: *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.*

- Action 3.2.1 Use the logon message to warn uninvited users that they are not allowed and to warn authorized users that they must use the system only for approved purposes. This action can be accomplished with the C2 Configuration Manager as well.
Hive: HKEY_LOCAL_MACHINE
Key: \Software\Microsoft\Windows NT\Current Version\Winlogon
Name: LegalNoticeText
Type: REG_SZ
Value: <enter a text message>

The LegalNoticeCaption value in the same key is the text that will appear in the title bar of the warning window. The sample banner from the Department of Justice may provide a starting point for your message:

WARNING! By accessing and using this system you are consenting to system monitoring for law enforcement and other purposes. Unauthorized use of this computer system may subject you to criminal prosecution and penalties.

By typing the legal notice in a text editor and then pasting it into the registry editor you can create a longer notice than allowed by directly typing into the registry fields. There are several other ways to add this logon message, e.g. the System Policy Editor, or the C2CONFIG.EXE or RREGCHG.EXE utilities in the NT Resource Kit. The Resource Kit can be purchased at any large bookstore. The Policy Editor has the advantage that the notice will be reapplied each time a user logs in, in case it gets removed.

- Action 3.2.2 If you use an FTP server, it should display a similar message. From the Start menu, go to Windows NT 4.0 Option Pack, Internet Information Server, and launch the Internet Service Manager utility. Go to the properties of your FTP site and enter your warning on the Messages tab.

PHASE 3

SETTING REGISTRY KEYS

STEP 3.3.

Disable floppy disk drives and hide drive letters.

Problem: *This problem was discussed in Phase 1. If you do not physically remove the drives then these Registry settings will disable or hide floppy disk drives and CD-ROM drives. Also, when the file AUTORUN.INF is present, the autorun feature of Windows NT executes programs automatically when the drive, such as a CD drive, is accessed. Hard drives and shares also have this feature. The commands in the AUTORUN.INF file could cause malicious programs to run when the drive or share is accessed.*

- Action 3.3.1 Use the *Resource Kit* service FLOPLOCK to lock access to the floppy drive. When used on Windows NT Workstation, this will restrict access to the floppy drive to Administrators and Power Users. When used on Windows NT Server, it will restrict access to the floppy drive to Administrators. These restrictions do not apply if the computer is booted into another operating system. See the *Resource Kit* help for the procedures to install FLOPLOCK. Using the default location of the NT Resource Kit, the command is: "instsrv FloppyLocker c:\ntreskit\floplock.exe"
- Action 3.3.2 Disable AutoRun on drives and shares.
Hive: HKEY_CURRENT_USER
Key: \Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Name: NoDriveTypeAutoRun
Type: REG_DWORD
Value: 0x0000007f

This value disables AutoRun for all drives and shares.
- Action 3.3.3 On workstations, hide those drives which users do not need to use, e.g., a CD-ROM drive, or the boot partition. To hide drives add the following value to the registry.
Hive: HKEY_CURRENT_USER
Key: \Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Name: NoDrives
Type: REG_DWORD
Value: <see right>

The value data is a 32-bit binary number, where the first 26 bits correspond to the drive letters Z through A. A 1 in a bit position means that the drive is hidden, whereas a 0 means it is visible. As an example, the mask 1000000000000000000000000011 would hide the Z drive and the A, B, & C drives. Note 1: The registry editor will truncate leading zeroes. Therefore, if you want to hide any drives, you must hide the Z drive. This is the drive that is set as the user's home share by default. Note 2: This setting is in the user's registry hive. Therefore, it is very difficult to add to existing user accounts. However, it can easily be added to the default user's hive and will then be automatically applied to all new accounts. You may also design your own System Policy template that will set this key for any user you designate. Note 3: Any drives specified as hidden will be hidden only in the Explorer interface and Save/Open dialogs using the standard Win32 API. They will be visible in File Manager (%systemroot%\System32\winfile.exe) and the Command Prompt (%systemroot%\System32\cmd.exe). Therefore, appropriate NTFS permissions should be set on those executables to prevent users from circumventing this control. Note 4 3.3.2 and 3.3.3 are applied to HKCU only, not system wide.

STEP 3.4.


Enforce strong passwords (Registry portion).

Problem: *Weak passwords are easy for an intruder to crack. We cover password settings in phase 4, but Service Pack 2 and later versions come with a service that can enforce complex passwords. This service will ensure that passwords are (1) at least 6 characters long, (2) contain characters from at least three of the following four groups: lower case letters, upper case letters, numbers, non-alphanumeric characters, and (3) passwords do not contain your user name or any part of your full name. These requirements are enforced the next time a user changes his or her password.*

- Action 3.4.1 Enable weak password filtering on the PDC (and any BDC that may be promoted) by installing the latest Service Pack and modifying the Notification Packages value in the registry. If this value is not present, create it with REGEDT32.EXE. If it already exists, take care to append the data below: do not overwrite the value's data or replace existing contents.

Hive: HKEY_LOCAL_MACHINE
Key: \SYSTEM\CurrentControlSet\Control\Lsa
Name: Notification Packages
Type: REG_EXPAND_SZ
Value: %systemroot%\system32\passfilt.dll

- Action 3.4.2 If Microsoft's password filter does not meet your needs, a custom filter can be written and installed instead. See the Knowledge Base article number Q151082 at <http://www.microsoft.com/technet> for details, and the Win32 SDK for sample code. Note that Service Pack 4 or later should be installed, since earlier versions do not inform users why their proposed new passwords fail. When password filtering is implemented, e-mail should be sent to all users explaining the complexity requirements as well. Note that there are also third-party password checking applications which provide more functionality, such as the Quakenbush Password Appraiser.

Caveat:  If an attacker can replace your filtering program file (PASSFIL.DLL) with his own, then this Trojan Horse program can save passwords in cleartext and/or send them to the attacker. Hence, assign permissions and audit access to the filtering program to prevent this. Periodically reinstall the file from a secure source to overwrite any undetected Trojan versions.

PHASE 3

SETTING REGISTRY KEYS

STEP 3.5.

Avoid the Netware DLL Trojan horse.

Problem: *The Local Security Authority uses a DLL to collect passwords for further authentication on a Netware server. This DLL is not installed in a default NT Workstation installation, even though the system will look for it. Therefore, users with write access to %systemroot%/system32 can install a Trojan DLL and collect passwords. This DLL is only necessary if the MS Netware client is being used. If not, then this DLL should be disabled in the registry by removing the call to it.*

- Action 3.5.1 Remove the entry FPNWCLNT (the Netware DLL) from the following Notification Packages value. Take care not to remove any other entries, such as PASSFILT.

Hive: HKEY_LOCAL_MACHINE
Key: \SYSTEM\CurrentControlSet\Control\Lsa
Name: Notification Packages
Type: REG_MULTI_SZ
Value: <remove FPNWCLNT, do not add or delete anything else>

STEP 3.6.

Secure print drivers.

Problem: *Some sites believe that printer drivers should be protected; for example, when blank check paper or purchase order forms are kept in the printers. If your site wants to protect print drivers, the following action will limit control of drivers to Administrators and Print Operators. Moreover, printer drives run at the highest privilege level (kernel mode), hence, Trojan Horse drivers are extremely dangerous.*

- Action 3.6.1 Add the following registry value:
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentcontrolSet\Control\Print\Providers\LanMan Print Services\Servers
Name: AddPrintDrivers
Type: REG_DWORD
Value: 1

Print Operators should not have access to the printer driver files. These files run in kernel mode and a Print Operator that cannot be trusted could gain administrative access to the system by installing a Trojan Horse driver. Therefore, make Administrators the owners of those drivers and set appropriate ACLs on them.

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 3


SETTING REGISTRY KEYS

STEP 3.7.

Enable audits of backups and restores.

Problem: *If an unauthorized user can restore files to a new directory, they can compromise those files. Audit all such actions. You need to limit who has access to the backup program, because users can use that program to steal files. Even if you grant users just read access to a file, they can back it up and steal it if they have access to the backup software.*

- Action 3.7.1 Set this registry value:
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\Lsa
Name: FullPrivilegeAuditing
Type: REG_BINARY
Value: 1

Caveat:  *This setting will cause a very large number of event records during backups and restores. Increase the size of the event log and (possibly) reset CrashOnAuditFail so the system will continue operating. NOTE: Action 5.1.3 describes how to increase the size of the event log.*

STEP 3.8.

Restrict anonymous logon.

Problem: *A “null user session” is a session established over the network with a blank username and blank password (it is not the same as the IIS anonymous account). Windows NT allows null user sessions to remotely download a complete list of usernames, groups and sharenames. Blocking this security hole is one of the most important changes you can make to your system.*

Note: If you have a multiple domain environment, or if you are using Novell’s NDS for NT or other applications that rely on null user sessions, then see Knowledge Base article number Q143474 at <http://www.microsoft.com/technet>.

- Action 3.8.1 Set this registry value. If it does not exist, then create it with REGEDT32.EXE.
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\LSA
Name: RestrictAnonymous
Type: REG_DWORD
Value: 1

Note: Under Service Pack 3, anonymous users could still obtain the password policy with this setting. Service Pack 4 fixes this vulnerability. The tools user2sid and sid2user will still work with RestrictAnonymous=1 set.

PHASE 3

SETTING REGISTRY KEYS

STEP 3.9.

Control remote access to the registry.

Problem: *REGEDIT.EXE, REGEDT32.EXE and POLEDIT.EXE can be used to access the registries of other computers over a network, including the Internet.*

- Action 3.9.1 Restrict network access to the registry by using REGEDT32 to change the permissions on the WINREG key in the registry. Whatever permissions exist for this one key will be interpreted by Windows NT as the permissions you desire for all remote access to any part of the registry.
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\
Control\SecurePipeServers\winreg

Give Full Control to the Administrators group and the System account. If you have applications that require null user session access to the registry, then give Read permission to the Everyone group. For more information, see Knowledge Base article number Q155363 at <http://www.microsoft.com/technet>.

STEP 3.10.

Restrict anonymous network access to the registry and other named pipes.

Problem: 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, including the pipe for the registry (which is named “winreg”).

- Action 3.10.1 Apply Service Pack 3 or later, and remove the names of any named pipes (such as “winreg”) which 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. Even removing “winreg” to prevent anonymous access to the registry may break certain applications.
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\LanManServer\Parameters
Name: NullSessionPipes
Type: REG_MULTI_SZ
Value: <Remove names from the list to prevent null session access to them.>

Service Pack 3 and higher should automatically remove the “winreg” entry for access to the registry. However, before making wide scale changes, test your modifications on a single system. Some applications may require anonymous access to the registry in order to function (for example, Cheyenne ARCServe 6.0).

Note 1: The above setting relies on another registry setting in order to work:

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Services\LanManServer\Parameters
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.

Note: A related setting restricts which shares a null session can connect to. This setting works similarly to NullSessionPipes and is called NullSessionShares. It resides in the same location in the registry.

PHASE 3

SETTING REGISTRY KEYS

STEP 3.11.

Control access to the command scheduler.

Problem: *The Schedule service is used to define when programs and batch jobs are automatically executed by the operating system, typically at recurring times or days. Any process launched by the Schedule service acts as a part of the operating system, and thus has unlimited power over the computer. If an attacker can list which jobs have been scheduled, the she could upload a Trojan Horse file to replace the file that will be executed. Another issue concerns how to allow others to submit jobs to the Schedule service without making them members of the Administrators or Power Users groups.*

- n Action 3.11.1 By default, only Administrators and Power Users can submit new jobs. To also allow Server Operators to submit jobs, then add the following value.
Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Control\Lsa
Name: SubmitControl
Type: REG_DWORD
Value: A value of 0 means that only Administrators and Power Users can schedule jobs. A value of 1 means that Server Operators may also schedule jobs.

- n Action 3.11.2 To list which jobs have already been scheduled, a user must have permission to access the registry key which contains this information. Hence, to control who can list existing jobs, use REGEDT32 to modify the permissions on the following key:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Schedule

PHASE 3

SETTING REGISTRY KEYS

STEP 3.12.

Secure the Registry.

Problem: *If registry settings are changed, security may be diminished. However, you cannot just lock up the registry because there are many valid reasons—generally associated with applications—why users would need to change the registry. Therefore, setting ACLs on parts of the registry is important. Unfortunately, it is difficult to know which registry ACLs to modify and there are a large number of keys requiring modification.*

- Action 3.12.1 Install Service Pack 4 or later, and obtain the new Security Configuration Manager (SCM) utility from Microsoft. The SCM includes a predefined template of registry ACLs which can be applied in one simple step. The SCM can be downloaded for free from <http://www.microsoft.com/ntserver>. Please see the help and readme files that accompany the SCM for instructions. If desired, registry permissions can also be modified by hand with REGEDT32.EXE by highlighting the key whose permissions need to be modified, then pulling down the Security menu and choosing Permissions. Be sure to test any settings thoroughly before rolling them out to production systems, whether those changes are made with the SCM or REGEDT32.

- Action 3.12.2 Ensure that the HKLM\Software\Microsoft\Windows NT\CurrentVersion\AEDebug key is adequately protected. The Authenticated Users group should be granted only Read and Execute permissions. This key controls what program is launched when a process crashes. By default, it is Dr. Watson. However, if this is changed, the program that gets launched has the same rights as the program that crashed. If someone is able to modify the AEDebug key and then crash a privileged program, they can launch any program they wish with elevated permissions.

- Action 3.12.3 Other specific registry keys to secure include:

HKEY_LOCAL_MACHINE:
\Software\Microsoft\RPC (and its subkeys)
\Software\Microsoft\Windows NT\ (and its subkeys)
\Software\Microsoft\Windows NT\CurrentVersion\Drivers
Embedding
Fonts
FontSubstitutes
GRE_Initialize
MCI
MCI Extensions
Ports (and all subkeys)
Profile List
WOW (and all subkeys)
\Software\Microsoft\Windows NT\Windows3.1MigrationStatus
(and all subkeys)

Set permissions on these keys so that the Authenticated Users group is granted only Read and Execute permissions.

HKEY_CLASSES_ROOT:
\HKEY_CLASSES_ROOT (and all subkeys)

HKEY_LOCAL_MACHINE:
\Software\Microsoft\Windows NT\CurrentVersion\Compatibility

Set permissions on these keys so that the Authenticated Users group is granted only Read, Write and Execute permissions.

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 3

SETTING REGISTRY KEYS

STEP 3.13

Block the 8.3 attack.

Problem: By default, NT automatically generates short 8.3-compatible (DOS) file names for files with long file names. If a user has access to a file which has the same first 8 characters and extension as a file the user does not have access to, access is possible to the other file by requesting it in 8.3 format.

- Action 3.13.1 Two values in the registry may need modification:
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\
Control\FileSystem
Name: Win31FileSystem
And
Name: NtfsDisable8dot3NameCreation
Type: REG_DWORD
Value: 1
The Win31FileSystem value pertains to FAT partitions, and the NtfsDisable8dot3NameCreation entry pertains to NTFS partitions. A value of 1 for either will disable the 8.3 naming system on partitions of that type. A value of 0 will enable it. Note: This may break certain older and/or poorly written applications which rely on the 8.3 naming convention. Caveat: The Win31FileSystem key may be spelled Win32FileSystem. This is fine. Do not worry about it.

STEP 3.14

Implement NTLM v2.

Problem: NTLM is a challenge/response authentication protocol used by Windows NT to prevent passwords from being sent over the wire in cleartext. However, because the protocol is weak, it is possible for attackers to extract password hashes from captured logon session packets and load them into password auditing tools, such as L0phtCrack, to reveal the cleartext passwords. NTLMv2, on the other hand, is a far superior protocol and L0phtCrack cannot extract password hashes from its sessions. NTLMv2 is available with Service Pack 4 or later. Domain controllers will support NTLMv2 simply by applying the Service Pack, but clients require a registry change. NTLMv2 can be required from either the server's or client's side of the authentication session.

- Action 3.14.1 Use NTLMv2 when possible. To enable NTLMv2 add the following registry value:
Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Control\Lsa
Value Name: LMCompatibilityLevel
Value Type: REG_DWORD – Number
Value Data: Valid Range: (0-5; Default Value: 0)

- Level 0 – Clients do not use NTLMv2. Domain controllers will accept LM, NTLM and NTLMv2 authentication.
- Level 1 – Clients attempt to use NTLMv2 if the Domain controller accepts it but will use LM or NTLM if needed. Domain controllers will accept LM, NTLM and NTLMv2 authentication.
- Level 2 – Clients attempt to use NTLMv2 if the Domain controller accepts it but will use NTLM if needed (clients will not use LM). Domain controllers will accept LM, NTLM and NTLMv2 authentication.
- Level 3 – Clients use NTLMv2 only. Domain controllers will accept LM, NTLM and NTLMv2 authentication.
- Level 4 – Clients use NTLMv2 authentication, and use NTLMv2 session security if the server supports it. Domain controllers will accept NTLM and NTLMv2 authentication.
- Level 5 – Clients use NTLMv2. Domain controllers will accept only NTLMv2 authentication.

Note: To ensure compatibility, NTLMv2 should be tested prior to widespread distribution.

PHASE 3

SETTING REGISTRY KEYS

STEP 3.15

Secure Netlogon Channel.

Problem: The NetLogon Channel is used for passthrough authentication, synchronization of the SAM directory database between the primary and backup domain controllers, and the creation of trusts between domains. However, only the computer account password is encrypted by default, and none of the data transmitted is checked for integrity, thus leaving the system open to man-in-the-middle attacks and packet sniffing. Beginning with Service Pack 4, the option is available to require digital signing and/or encryption of all NetLogon Channel traffic.

- Action 3.15.1 To secure NetLogon Channel, add the following registry value:
Hive: HKEY_LOCAL_MACHINE
Key: \system\CurrentControlSet\Services\
netlogon\parameters
Value Name: See Table Below
Value Type: REG_DWORD
Value Data: 0 (False) or 1 (True)

Value Name: SignSecureChannel – Specifies that all outgoing secure channel traffic should be signed. NOTE: Setting the value SealSecureChannel to TRUE will override any setting for this parameter and force it to true.

Default Value: TRUE.

Value Name: SealSecureChannel – Specifies that all outgoing secure channel traffic should be encrypted.

Value Name: RequireSignOrSeal – All outgoing secure traffic must be either signed or sealed.

NOTE: If this value is not set, integrity checking is negotiated with the Domain Controller. Only set this value to true if ALL of the domain controllers in ALL trusted domains support signing and sealing. If this value is set to TRUE, SealSecureChannel is implied to be TRUE.

STEP 3.16

Mitigate the Risk of Syn Flood attacks.

Problem: A standard TCP connection is established by a three-way handshake between two systems. The system requesting the connection sends a SYN packet to the destination host. The destination host replies by sending a SYN/ACK packet to the requesting system. The requesting system then sends an ACK packet to complete the connection. The destination host will allocate CPU cycles and memory to the connection once the SYN/ACK packet is sent. If no ACK package is received, the destination host will resend the SYN/ACK packet on a regular interval until the request times out. In a SYN Flood attack, the target receives thousands of SYN packets but no corresponding ACK packets, consuming system resources with incomplete connections.

- Action 3.16.1 Beginning with Service Pack 5, a Registry value can reduce the number of SYN/ACK retries and control the amount of resources committed to incomplete connections. Add a new registry value as follows:
Hive: HKEY_LOCAL_MACHINE
Key: \SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Name: SynAttackProtect
Type: REG_DWORD
Value: 2

Possible values are:

- 0 – Offers no protection (this is the default value)
- 1 – Reduces the number of SYN/ACK retransmissions
- 2 – Reduces the number of SYN/ACK retransmissions and requires the completion of the three-way handshake before additional resources are committed to the session

Note: This setting reduces but does not eliminate the risk of a successful SYN Flood Attack.

PHASE 4


ESTABLISH STRONG PASSWORD CONTROLS AND SECURE ACCOUNT POLICIES

STEP 4.1.

Lockout attempts to gain access after a set number of attempts and make passwords hard to guess.

Problem: *The default configuration allows “door knocking” penetration of user accounts, a common computer system penetration technique in which an intruder attempts to logon as an authorized user. Insecure settings allow multiple repeated attempts without either logging failed attempts or disabling accounts after a set number of failed attempts. Foil any but the luckiest door knocking penetration by making passwords hard to guess and enabling automatic lockout of non-administrator accounts after a number of failed login attempts.*

- Action 4.1.1 In the User Manager, set a password for each new account, enable “User Must Change Password at Next Logon,” (this is enabled by default any time an administrator sets a password for another user) and disable “Password Never Expires.” (Important warning: If you set “User Must Change Password” and, in 4.1.3 below, “User Must Logon to Change Password,” the user may not be able to log on the first time. So enable “User Must Change Password” until they have signed on one time and then disable it and enable “User Must Logon to Change Password.”)
- Action 4.1.2 Ensure that all accounts have passwords. This won’t be an issue if you are setting up a new system and give each account a password, but may be a required action if you are taking over an existing system.
- Action 4.1.3 To make passwords hard to guess and force users to change them frequently, in User Manager, Policies menu, Account window make the following settings:
 - Maximum Password Age = 45 - 90 days
 - Minimum Password Age = 1-5 days
 - Minimum Password Length = 8 characters
 - Password Uniqueness = 8 - 13 passwords
 - Account Lockout - lockout after 5 attempts; reset count after 4 hours
 - Lockout Duration - 4 hours (or forever if you want to force an administrator to unlock it).
 - Users Must Logon to Change Passwords = yes

Caveat:  If you set it to yes on a Citrix or similar server, users may not be able to logon without changing their passwords. If a range is shown, choose a value that you like within that range.

Note 1: Longer lockouts enable a different kind of denial-of-service attack in which attackers can force users to be locked out of their workstations.

Note 2: The consistent enforcement of the password policies depends on the clients, e.g., with Windows 9x clients, the “Account Lockout,” “Lockout Duration,” and “User Must Logon to Change Passwords” might not be enforced.

PHASE 4

ESTABLISH STRONG PASSWORD CONTROLS AND SECURE ACCOUNT POLICIES

STEP 4.2.

Enable Administrator account lockout, and rename the Administrator account.

Problem: *The Administrator account cannot be locked out using the methods of step 4.1. That makes the most critical account more vulnerable to repeated cracking attempts than less critical accounts.*

- Action 4.2.1 Install the PASSPROP.EXE utility included in the NT *Resource Kit*. Passprop locks out the Administrator account after repeated failed access attempts over the network, but never locks the Administrator account out at the console.
- Action 4.2.2 Rename the Administrator account to some other name. This will not stop smart attackers, who can find the Administrator account through a null logon, but great security is a series of walls that the enemy must climb, and renaming the Administrator account is another (small) wall. Simply create a new user and make them a member of the Administrator group.
- Action 4.2.3 Create a bogus account called Administrator without administrative privileges. This might stall an attacker temporarily. You can also put a logon script on this account which auto-dials a pager to the Administrator to alert of a break-in. The logon script will only run if the user logs on from the Ctrl-Alt-Del login box. You will not be notified if the user authenticates as the bogus Administrator from a command prompt.

STEP 4.3.

Establish separate accounts for Administrators.

Problem: *Administrators sometimes leave their accounts logged on; they're only human. Since administrative accounts have extraordinary privileges that practice could be dangerous.*

- Action 4.3.1 Give Administrators a separate personal account, in a group that has normal privileges, for their use when not performing tasks requiring the Administrator account.

Note: Administrators can use the SU utility in the Resource Kit to quickly change contexts so that they can perform administrative tasks without having to log off and log back on using the Administrator account.

STEP 4.4.

Set up an Administrator password control process.

Problem: *The built-in Administrator account cannot be deleted and, by default, cannot be disabled due to bad logon attempts. Hence, attackers will attempt to guess its password. Conversely, if the password is forgotten, it will be inconvenient to recover or reset it. With physical access to a domain controller, one can reset the Administrator password by booting from a floppy with special utilities, or the password can be recovered by cracking it with *LOphtCrack* (www.l0pht.com) or the *Quakenbush Password Appraiser* (www.quakenbush.com).*

- Action 4.4.1 Seal the built-in Administrator account password in an envelope and lock it up. When needed, use the password and change it before locking it up again. Of course, this procedure is based on your not using the default Administrator account other than in emergency situations. For day-to-day administrative activities, create additional user accounts and add them to the local Administrators group.
- Action 4.4.2 Set the "Password Never Expires" option for the built-in Administrator account. This will alleviate the problem of having to update the locked up password each time the password expires.
- Action 4.4.3 Use extended ASCII characters (Hold down the ALT key and type the character code using the numeric keypad) in the password for this account. Though difficult to type, these characters are not usually included in the character sets for password cracking programs.

PHASE 4

STEP 4.5.

Tighten the use of the Everyone group and disable the guest account.

Problem: The “Everyone” group on NT systems includes literally everyone, even anonymous users from the Internet without user accounts. Hence, permissions granted to Everyone are permissions that hackers enjoy as well. Once a resource is protected from the Everyone group, an attacker is likely to attempt to log on with the Guest account since it is built-in and cannot be deleted.

Note: Do not deny access to the everyone group. If you do this essentially everyone including administrators will be denied access.

- Action 4.5.1 In general, the permissions on NTFS folders and shared folders should be set to the following as a starting point, and then modified as necessity requires. The goal is to remove the Everyone group from the permissions list, but still retain usefulness and convenience without compromising security. Note that the CREATOR/OWNER group is not visible in User Manager, but permissions can be assigned to it when modifying ACLs in Windows Explorer or REGEDT32. All resources and objects in Windows NT have “owners”, which is initially set to the person who created the item. Hence, the CREATOR/OWNER group is equal to *whoever* is the current owner of the object or resource. Ownership can change, but the ACL need not be modified. The default permissions should be:
 - Authenticated Users: Change
 - CREATOR/OWNER and Administrators: Full Control

- Action 4.5.2 Disable the guest account in User Manager by double-clicking it and checking the “Disable Account” box. It is disabled by default in Windows NT Server 4.0, but if you have a previous version, NT Workstation, or if you have enabled guest access, disable it. Also, add a password to the Guest account in case it is accidentally enabled. Consider renaming the guest account.

STEP 4.6.

Avoid giving Administrator privileges for most tasks.

Problem: Permissions are virtual doors through which people can come and go and remove or destroy or change information and programs. Some of the worst problems are caused by well-meaning people who simply make mistakes. Giving in to user demands for Administrator privileges can create grave security and reliability problems. However, when administrators run into problems in which applications do not run, they sometimes give up and allow everyone to gain access to files and registry elements that should be protected.

- Action 4.6.1 Use less privileged accounts when people ask for Administrator privileges. For example, for desktop maintenance people, create a group such as “desktop” and add the rights they need (i.e., “add workstation to the domain”). Place all desktop support personnel in this group with their own user IDs and passwords. Push this group to local admin. on each workstation. Now they can do their job WITHOUT sharing a DOMAIN Administrator password. Similarly allow system operators to submit AT commands. You may also want to investigate third-party utilities to ease these administrative tasks.
- Action 4.6.2 Avoid Full Control permissions for Everyone (or Authenticated Users) and limit Change access to users who need to delete and/or modify files and directories. In particular, avoid assigning Change and Full Control permissions for system directories—particularly %systemroot%, winnt, winnt\system, winnt\system32, and winnt\system32\config. In addition, avoid permissions for Everyone (or Authenticated Users) on settings in each host’s registry wherever possible.

PHASE 4

ESTABLISH STRONG PASSWORD CONTROLS AND SECURE ACCOUNT POLICIES

STEP 4.6. continued

- Action 4.6.3 Tighten security on critical files. These include:
 - %systemroot%\profiles directory
 - Temp directories (typically c:\temp but possibly also %systemroot%\tmp)
 - Audit logs (%systemroot%\system32\config*.evt) (see next step)
 - Registry files (%systemroot%\system32\config, also backed up to %systemroot %\repair)
 - %systemroot%\system32\ntbackup.exe
 - rdisk.exe - rsh.exe
 - regedit32.* - telnet.exe
 - rcp.exe - tftp.exe
 - rexec.exe - ftp.exe
 - %systemroot%\regedit.exe
 - All executables
 - All shared directories
 - Boot files on the System Partition:

On Intel platforms:

- BOOT.INI
- NTLDR
- NTDETECT.COM
- Eventually NTBOOTDD.SYS and BOOTSECT.DOS

On Alpha platforms:

- OSLOADER.EXE
- HAL.DLL

The autoexec.bat and config.sys files are mostly not used in NT and can be safely removed. NT uses two files, called config.nt and autoexec.nt, located in the %systemroot%\system32 folder, to initialize the DOS environment for DOS and 16-bit Windows apps. These files also need appropriate protection. Some NT experts recommend that device drivers (*.drv), screen savers (*.scr), system files (*.sys), command scripts (*.cmd) and ActiveX controls (*.ocx) be added to the list of critical files. Software products such as IIS and Exchange add a number of critical files to the operating system and these files also require greater security savings.

STEP 4.7.

Secure and Manage Event Logs.

Problem: Windows NT's event logs need to be secured. By default, only someone with the "Manage Security And Audit Log" privilege has permissions to the SECEVENT.EVT file (the security event log). The other logs may be accessed by a user with ordinary privileges. This does not provide sufficient security in most situations.

- Action 4.7.1 Use less privileged accounts when people do not need more privileges. Do not give any regular user the right to "Manage Security and Audit Log" in User Manager. A regular user with that right can empty the security log without an entry being made recording that event.
- Action 4.7.2 The log files are stored in %systemroot%\system32\config*.evt. It is prudent to copy these to a different computer at regular intervals to guard against data loss, and to ensure availability for legal or investigative purposes.
- Action 4.7.3 Set the NTFS permissions on the event log files to allow only Administrators and System access.
- Action 4.7.4 Turn on auditing for the event log files since there is no way to know whether they have been copied or viewed without auditing.

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 4

STEP 4.8.

Avoid using shared accounts—along with an exception.

Problem: Shared accounts greatly reduce the accountability of individual users who share a single account.

- Action 4.8.1 Avoid the use of shared accounts if at all possible. Limit the user environment in shared accounts to the bare minimum necessary. This can be done through the policy editor or logon scripts. In addition, give departments shared directories to avoid the need for sharing accounts.
- Action 4.8.2 An Exception: If you are in a manufacturing environment, and feel that shared accounts are absolutely necessary for efficiency on the plant floor, strictly limit their privileges and, if possible, restrict the workstations on which they can be used.

STEP 4.9.

Run an ACL reporting tool.

Problem: Most administrators find it difficult to monitor access control lists on all accounts. But monitoring is essential for maintaining confidence in security.

- Action 4.9.1 Run a reporting tool against both Administrator and user accounts (looking for null passwords, no passwords required, group memberships in the Administrator's group, etc). Examples of such tools are the Microsoft Security Configuration Manager (www.microsoft.com/ntserver), the Pedestal Software DACL and SACL command-line utilities (www.pedestalsoftware.com), and BindView NOSadmin for Windows NT (www.bindview.com).

STEP 4.10.

Encrypt the SAM password database with 128-bit encryption.

Problem: NT stores passwords in the Security Account Manager database. Although the SAM protects these passwords, password crackers can still be used to obtain valid passwords.

- Action 4.10.1 Apply Service Pack 3 or later, then run the SYSKEY.EXE utility. SYSKEY allows 128-bit ("strong") encryption of passwords in the SAM. Do this on all domain controllers. A thorough discussion of SYSKEY is beyond the scope of this document, but readers are referred to Knowledge Base article Q143475 at <http://www.microsoft.com/technet>. SYSKEY is mainly for environments with very high security needs. There is no uninstall option for SYSKEY! If you do enable the SYSKEY solution, you need to initiate measures for key recovery in case your key is lost or degraded.

STEP 4.11.

Set Appropriate User Rights.

Problem: Permissions, such as read, write, and execute, define the abilities of users to access certain objects such as folders or files. User rights, such as Log on locally, and Access this system from the network, apply to the system as a whole and are set separately from permissions. It is important to note that rights can override permissions. For example, a user with the right to restore files and directories can restore those files for which s/he has no read or write permissions.

- Action 4.11.1 Rights are separated into two categories: Standard Rights and Advanced Rights. Standard Rights are commonly given to users and control how the user can access or interact with the system. Advanced Rights allow very high-level access to the system and should not usually be given to users or groups.

To set user rights, open User Manager for Domains, and click on Policies/ User Rights. The Standard User rights are listed in a drop-down box. To also show the Advanced User Rights, mark the check box at the bottom of the dialog box. Selecting a right will show the current groups assigned the right and allow you to add or remove the right from other groups. Though you can grant rights to specific users, like permissions, rights should be assigned to groups, not to individual users.

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 4 ESTABLISH STRONG PASSWORD CONTROLS AND SECURE ACCOUNT POLICIES

STANDARD RIGHTS				
<i>Right</i>	<i>Possible Problems</i>	<i>Domain Controller</i>	<i>Member Server</i>	<i>Workstation</i>
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.	None	None	
Access 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 this right from the administrator accounts)	Domain Users	None
Backup Files and Directories	Users with no permissions for certain files or folders can still 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; A special group can be created to separate this right from the restore right.	Backup Operators; A special group can be created to separate this right from the restore right.	Backup Operators; A special group can be created to separate this right from the restore right.
Change the System Time	Resetting the system time can seriously impact or destroy audit trails.	Administrators	Administrators	Administrators; Power Users
Log on Locally	Known security bugs (such as GetAdmin) can escalate users permissions if run from the local console.	Administrators; Server Operators; Backup Operators	Administrators; Server Operators; Backup Operators	Administrators; Users
Manage Audit and Security Logs	Allows viewing and clearing of the audit logs. An attacker could clear the security log to erase evidence of the attack.	Administrators	Administrators	Administrators
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; A special group can be created to separate this right from the backup right.	Backup Operators; A special group can be created to separate this right from the backup right.	Backup Operators; A special group can be created to separate this right from the backup right.
Shut Down the System	Users could bring the system down in the middle of critical jobs or while users are accessing system resources.	Administrators; Server Operators	Administrators	Administrators; Users
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

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 4 ESTABLISH STRONG PASSWORD CONTROLS AND SECURE ACCOUNT POLICIES

ADVANCED RIGHTS

<i>Right</i>	<i>Possible Problems</i>	<i>Domain Controller</i>	<i>Member Server</i>	<i>Workstation</i>
Act as Part of the Operating System	Acting as part of the operating system overrides all other rights, permissions, or privileges.	None	None	None
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; Backup Operators	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
Debug Programs	Allows the user to debug processes and threads. Users with this right could modify programs to run malicious code.	Administrators	Administrators	Administrators
Increase Scheduling Priority	This allows a user to increase the priority of a process in NT. Setting a process's priority to 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 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
Modify Firmware Environment Variables	Environment variables can be modified to point to malicious programs	Administrators; Server Operators; Backup Operators	Administrators	Administrators
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

STEP 5.1.

PHASE 5

Turn on auditing.

AUDITING

Problem:

Knowing quickly that an attack has occurred and intervening is extremely important. In addition, it is important to keep in mind that the major security threats in Windows NT are Denial of Service attacks. Therefore, managing audit logs is critical. When Windows NT audit logs fill up, NT can either (a) erase old information and continue operating, or (b) halt. If you allow NT to continue operating, you may lose important information and/or an intruder can cause the log to fill up with extraneous information to hide evidence of his actions.

- Action 5.1.1 Turn on event auditing. To enable Event Auditing, open User Manager, pull down the Policies menu and choose Audit. Select the “Audit These Events” radio button. Choose the events to audit according to your security policy. The policy should include, at a minimum: Logon and Logoff, success and failure, File and Object Access, failure, Use of User Rights, failure. Security Policy changes, success and failure, Startup, Shutdown, and System, success and failure. Caveat: File and Object Access failure auditing can generate a very large number of entries. Therefore, it is recommended to set up auditing in the file system only for those files for which this information is important.
- Action 5.1.2 Set up file, RAS, printer and registry auditing as your site policy requires. Caveat: Log size can grow very fast when file auditing is enabled. One company reported 10,000 audit events recorded every 60 seconds on one server.
- Action 5.1.3 In Event Viewer, pull down the Log menu and use the Log Settings... option to set the log file size very large to avoid running out of log space while setting up the system and the audit policy. After the system has been operating properly for a few weeks, the file size can be reset to a more conservative value while still minimizing the possibility of overwriting unsaved log data. If you make a full backup once a week, choose “Overwrite Events As Needed” since you already have a backup of the old events.
- Action 5.1.4 Save the audit files daily in both event format and in comma-separated-value format for later analysis. This allows them to be saved automatically during back-up. Caveat: Do not choose “Clear log manually” unless necessary since it can cause the system to halt, causing Denial of Service.
- ▲ Action 5.1.5 (Advanced) In some very high security settings, the administrator may decide the risk of crashing the system is less than the risk of losing event log information. In these cases, CrashOnAuditFail may be enabled. If enabled, the system will shut down when the event logs are full and only administrators will be allowed access to the system. To enable CrashOnAuditFail, add the following registry value:
Hive: HKEY_LOCAL_MACHINE
Key: \SYSTEM\CurrentControlSet\Control\LSA
Name: CrashOnAuditFail
Type: REG_DWORD
Value: 1

To restart the system an administrator must reboot the server, log on and archive the event log, reset the registry value (it is reset to 2 when the system crashes due to full event logs), and reboot the system. *Caveat:* If enabled, attackers can use CrashOnAuditFail as a denial of service attack.

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 5 AUDITING

STEP 5.2.

Monitor the audit logs.

Problem: *If you don't see the problem, you cannot fix it.*

- Action 5.2.1 Set a regular schedule for examining security event logs for failed login attempts.
- Action 5.2.2 Use a third-party filtering and analysis tool. At the SANS web site (www.sans.org) there is a webcast on the use of NTLast. Additional tools are available at www.foundstone.com.
- Action 5.2.3 Use centralized monitoring. If a hacker is attacking a machine in Cleveland and you are in Boston, only centralized monitoring tools will warn you in time to act. Most host-based intrusion detection products include centralized monitoring, such as Centrax (www.cybersafe.com) and SystemScanner (www.iss.net).

Caveat: *The user assigned to a user account may not necessarily be the one abusing the system.*



STEP 6.1.

Turn off all unneeded network services and run needed services safely.

Problem: *Each network service you support creates two potential security problems: (1) they may open unknown (or known and unprotected) holes and (2) they may be useful in helping intruders attack other parts of the system. In addition, vulnerability in one machine can turn into vulnerability across an entire domain.*

- Action 6.1.1 Turn off all network services that you do not need, e.g. IIS, Peer Web Services, RAS, GOPHER, FTP, IP Forwarding, Simple TCP/IP Services, SNMP. Disable unneeded network protocols, e.g. TCP/IP, IPX, or NetBEUI. In addition, disable Server, Alerter, and Messenger services, where appropriate. In addition, do not allow users to install additional network services. This also means that you should keep the distribution CDs stored in a secure location and not copy the distribution files onto the users' harddrives. Note: The SNMP service can be used by an attacker to gain information, such as user accounts, available shares, etc. from an NT system because of lax default permission settings. If you need to run the SNMP service, ensure that you: (1) install Service Pack 4, (2) do not use the default community name (public), and (3) configure all communities as read only.

PHASE 6

NETWORKING AND INTERNET SECURITY SETTINGS

- Action 6.1.2 Verify that the services you are running are the latest versions. This means installing the latest Service Packs and hotfixes from Microsoft, and obtaining the latest upgrades to the services (such as IIS) installed.
- Action 6.1.3 If at all possible, refrain from using domain accounts for services. Domain accounts are the standard accounts used for users and administrators in a domain. Many services require a domain administrative account to run. Normally, it is more secure to run services in the SYSTEM context. However, certain services, such as domain backup software, require the use of domain accounts. Using domain accounts for services can turn a single-machine vulnerability into a domain-wide vulnerability since anyone with administrative privileges will have access to the password and user name of the service account. Service accounts are configured mainly through the Services icon, Control Panel.
- Action 6.1.4 Make sure that local accounts with the same name on different machines use different passwords. If account names and passwords are the same, NT sets up implied trust relationships and increases vulnerability. Educate users about the vulnerabilities they create with same name/password accounts.

STEP 6.2.

PHASE 6

NETWORKING
AND INTERNET
SECURITY
SETTINGS

If you use Internet Information Server (IIS), block known vulnerabilities.

Problem: *Web servers are magnets for intruder attacks - both simple and sophisticated. No part of the NT environment has shown up more often in the SANS Network Security Digest. Extreme care should be taken with IIS, both in configuration and in monitoring and installing patches. Microsoft has published a checklist for securing IIS. It is available at <http://www.microsoft.com/technet/security/iischk.asp>.*

- Action 6.2.1 Do not install IIS on a domain controller, except for decoy or honeypot purposes. If possible, make the IIS server a stand-alone instead of a member server, i.e., instead of a member of a domain. Otherwise, the IUSR_*computername* account is placed in the Domain users group allowing access to other platforms in the domain. Certain web-based applications may require that the IIS server be a member of a domain however.
- Action 6.2.2 Place the Web Server in the DMZ and use the external router to control the Internet traffic. From the external router, block all unneeded ports. Open only Port 80 if you are using only the web server; open port 443 if you are using a secure server.
- Action 6.2.3 Do not install a printer on the IIS machine. Computers in the DMZ should not be used for printing. If you MUST install a printer, apply all relevant patches for the spooler service.
- Action 6.2.4 Install the web folders on a drive other than the system drive.
- Action 6.2.5 Numerous exploits exist for the IIS sample pages. The Admin scripts directory allows extensive administration via Visual Basic Scripts. These should be taken off the system or moved and secured to prevent exploit.
Default locations for some of sample files are:
C:\inetpub\iissamples
C:\inetpub\iissamples\SDK
C:\inetpub\AdminScripts
C:\Program Files\Common Files\System\msadc\Samples
- Action 6.2.6 Remove the virtual directory \Iisampwd. This is a sample application that allows passwords to be changed via the Internet. This page allows brute force attack against the system user accounts.

- Action 6.2.7 Move, rename, or delete any command-line utilities. These tools are usually found in the Winnt or Winnt\System32 directories. Common tools include:

arp.exe	ipconfig.exe	regedt32.exe
at.exe	nbtstat.exe	rexc.exe
atsvc.exe	net.exe	route.exe
cacls.exe	netstat.exe	rsh.exe
cmd.exe	nslookup.exe	runonce.exe
cscript.exe	ping.exe	secfixup.exe
debug.exe	posix.exe	syskey.exe
edit.com	qbasic.exe	telnet.exe
edlin.exe	rcp.exe	fttp.exe
finger.exe	rdisk.exe	tracert.exe
ftp.exe	regedit.exe	wscript.exe
		xcopy.exe

- Action 6.2.8 Apply the very latest Service Packs and hot fixes for IIS. Refer to the Microsoft Security Advisor at <http://www.microsoft.com/security/> for notices.
- Action 6.2.9 Disable unnecessary services and features. The following services are typically not needed on a production IIS server, but, as always, testing is necessary: Alerter, ClipBook Server, Computer Browser, DHCP Client, Messenger, Netlogon, Network DDE, Network DDE DSDM, Network Monitor Agent, Simple TCP/IP Services, Spooler, NetBios Interface, TCP/IP NetBios Helper, NWLink NetBios, and the Server service. Also, disable the binding between the external interface and "WINS Client (TCP/IP)"; this is done on the Bindings tab in the Network applet, Control Panel. Remove the Jet and text ODBC drivers if these are installed. NOTE: After removing the WINS binding, Net BIOS name resolution will no longer function over the external interface.

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 6

NETWORKING AND INTERNET SECURITY SETTINGS

- Action 6.2.10 Disable .htr mapping if it is not needed. Htr scripts allow the manipulation of Windows NT passwords via IIS. If this functionality is not needed, it should be removed.
- Action 6.2.11 The Microsoft Data Access Components (MDAC) can be exploited to perform privileged actions. This functionality should be deleted unless specifically needed. If needed, be certain to upgrade to the latest MDAC version. To fully disable, perform the following steps: Delete the /msadc virtual directory from the default Web site Remove the following registry keys (if present) from the IIS Server

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\VbBusObj.VbBusObjCls

- Action 6.2.12 Secure the anonymous IIS account (*IUSR_computername*). Use a local account unless a web-based application requires a domain account. Assign the account a long and random password and remove the “Log On Over The Network” right for it in User Manager (the anonymous account does require the “Log On Locally” right, however). Rename the anonymous account, then create a new account with the prior name (*IUSR_computername*) and disable it.
- Action 6.2.13 Make sure the *IUSR_computername* account does not have write access to any files on the system. Also make sure the Creator_owner login does not have permission to any of the web files.
- Action 6.2.14 Disable parent Paths. Parent Paths allow you to send the notation ../ to the webserver causing it to go back up one directory. This may allow someone to get out of the web root and access system files if they can determine the directory path. If this must be enabled, be sure to keep the web contents on a secondary drive and use strong NTFS permissions.

To disable Parent Paths, Right-click the root of the web site, choose PROPERTIES; HOME DIRECTORIES, CONFIGURATION; APP OPTIONS and uncheck ENABLE PARENT PATHS.

- Action 6.2.15 Take advantage of IP address restrictions to block access from undesired domains or address ranges. IP address domain blocking is configured on the Security tab of the Properties of the website in the Internet Services Manager utility.
- Action 6.2.16 When user authentication is required, use either Challenge/Response authentication or Basic authentication with SSL encryption. Never use Basic authentication without SSL encryption because passwords are sent in clear text. The Challenge/Response authentication method can also use SSL encryption for another layer of security. Keep in mind that most browsers support Basic authentication, including Netscape Navigator, but only Microsoft Internet Explorer supports Challenge/Response authentication.
- Action 6.2.17 Never assign both the Write and Script/Execute permissions to the same folder. This will allow an attacker to upload a script or program and then remotely execute it on the IIS server.
- Action 6.2.18 Use the Script permission for Active Server Pages and CGI scripts. The Execute permission is only for binary executables. Place the scripts in a folder separate from the script interpreter. This scripts folder does not necessarily require the Read permission, depending upon the configuration.
- Action 6.2.19 Use NTFS on all IIS hard drives. IIS enforces NTFS permissions on the file system when serving pages to the Internet. Apply NTFS permissions against the *IUSR_computername* account to control anonymous access. User authentication is required (Basic or Challenge/Response) when using NTFS permissions with legitimate, non-anonymous users. (*continued*)

PAGE 33

PHASE 6

NETWORKING AND INTERNET SECURITY SETTINGS

When IIS permissions —such as Read, Write, Script and Execute— conflict with NTFS permissions, the more restrictive of the permissions in the conflict is the one that is enforced.

- Action 6.2.20 Enable W3C Extended logging to keep detailed records of client-server interaction. Use a scheduled batch script or other mechanism to periodically copy the log files off of the IIS server to a secured location.
- Action 6.2.21 Disable directory browsing, especially on folders containing scripts or executable.
- Action 6.2.22 Unless absolutely required, uninstall the HTML version of the Internet Service Manager utility. This is done with the IIS Setup program. If the HTML-ISM is required, then apply all possible protections for it: authentication, SSL, IP address restrictions, etc..
- Action 6.2.23 When using FTP, be aware that this service has suffered numerous security penetrations in the past and that passwords are always sent in clear text. Hence, only anonymous access should be allowed.
- Action 6.2.24 Avoid allowing FTP upload or write privileges. If they are necessary, the upload folders should be on a separate volume from the operating system.
- Action 6.2.25 FTP servers should have a relatively short connection time-out period, and a limited number of simultaneous sessions. These curtail certain Denial of Service attacks.
- Action 6.2.26 Consider using Virtual Private Networking technologies along with FTP when FTP is necessary, such as IPsec, L2TP or PPTP with MS-CHAPv2. An alternative is to use HTTP version 1.1, which allows uploading files with the HTTP protocol (recent browsers support this version of HTTP).
- Action 6.2.27 If at all possible, do not install the Microsoft FrontPage Server Extensions and do not allow users to manage their personal web sites with FrontPage. If these Server Extensions are necessary, ensure that you have installed the very latest version from <http://www.microsoft.com/frontpage/>. Refer to the *FrontPage Resource Kit* for detailed guidelines for the secure use of FrontPage.
- Action 6.2.28 Do not install Microsoft Index Server if it will not be used. However, this free IIS add-on is immensely useful and powerful. When used, only index those folders whose entire contents are happily accessible to the public. Do not index the entire hard drive, operating system folders, or scripts/executables folders. Recall that Index Server respects NTFS permissions, hence, queries cannot be used to access (or even see) files to which the user does not have NTFS Read permission. Use IP address restrictions to limit access to intranet users if desired. Consider creating multiple Index Catalogs with different contents and permissions: one for public access, another for intranet access.
- Action 6.2.29 Web application security is beyond the scope of this document, but a few guidelines can be mentioned: 1) only use scripts and applications whose source code you have checked yourself, 2) do not allow user input to be passed to system calls, 3) validate and error-check user input with robust exception-handling code, and process the input with dynamically allocated buffers, and 4) prefer out-of-process ISAPI applications running in their own address spaces over in-process applications. This last tip will make the ISAPI application run as slowly as a CGI script, but the IIS server will be more likely to survive a crashed web application. If you are not the web application developer yourself, you can assist by attempting to “break” the application as hackers do, e.g., by overloading the input strings, using non-standard input, telnetting into HTTP, issuing thousands of simultaneous requests, interrupting browser-server communications, modifying or deleting browser cookies during open sessions, etc.

STEP 6.3.

Protect vulnerable ports through a firewall (or screening router).

Problem: *The number of attacks in which a service available through these ports can be exploited has increased dramatically over the last year. NetBIOS and the Server Message Block (SMB) network is accessible by outsiders. The native Windows NT network protocol, SMB, can be accessible via User Datagram Protocol (UDP). TCP/IP and UDP/TCP/IP are the native network protocols of the Internet. The local SMB network may be accessible to everyone on the Internet. At least through Service Pack (SP) 2, NT Server 4.0 is vulnerable to a denial of service attack through its TCP/IP service on various ports (File and Print services on port 135, the netinfo service on port 1035 and DNS on port 53). An improper connection causes the server's processor utilization to go to 100%. This causes sluggish response to any other processes and disruption to some other network services it is running.*

- Action 6.3.1 Block TCP and UDP on ports 135 (RPC), 137 (nbname), 138 (nbdatagram) and TCP on port 139 (nbsession) at the gate to networks (and possibly also subnets) in which Windows NT runs. Block them as close as you can to NT to discourage internal attacks. Some sites reported grouping their NT servers in a single subnet or computer room. However, this is not always possible if, for example, a workstation needs access to a shared directory or when BackOffice is running. In those cases, at a minimum, block access to these ports with a firewall at the connection to the Internet. Remember to block both incoming and outgoing use of the ports as older versions of Internet Explorer report password and account information through these ports. Note: Blocking these ports (especially 135 UDP and 139 TCP) can disrupt authentication. Test this before you implement it in production. In addition, blocking these ports will block Windows Networking over NetBT (NetBIOS over TCP/IP). If you need to use NetBT then block these ports at the perimeter past which NetBT should no longer be allowed.
- Action 6.3.2 Many security vulnerabilities were corrected in recent Service Packs. Be sure to install the latest Service Packs relevant to your installation. (We'll repeat this later; important concepts bear repeating.)

PHASE 7


OTHER
ACTIONS
REQUIRED
AS THE
SYSTEM
IS SET UP

STEP 7.1.

Require password-protected screen savers on all workstations.

Problem: *Users sometimes leave their desks while their accounts are active, allowing anyone who passes by to gain access and impersonate the user.*

- Action 7.1.1 Provide all users with password protected screen savers and require that they set the delay before the screen saver comes on to 10 or, at most, 15 minutes.
- Action 7.1.2 Teach users to press Ctrl-Alt-Del and then "Lock Workstation" whenever they leave their workstations so that the lockout will go into effect immediately.

Caveat:  *If users do not complete the actions in 7.1.2, the lockout does not go into effect immediately. If users are unaware that there is a delay, they may have a false sense of security.*

PHASE OTHER ACTIONS REQUIRED AS THE SYSTEM IS SET UP

STEP 7.2.

Implement virus protection software.

Problem: *Viruses are a large and growing threat. It's possible that every server and workstation within a domain can be infected by a virus that was introduced via a single host.*

- Action 7.2.1 Install on-access virus scanning software on all workstations. Install software that searches for and eradicates viruses on all servers. Set a regular scanning schedule, or use on-access scanning. Note, however, that on-access scanning can be resource intensive and a trade-off may need to be made between security and availability.
- Action 7.2.2 On heavily-used servers, where on-access and/or full scanning is too resource intensive, concentrate scans on sensitive areas. These include user directories and anywhere else where users have Full Control or Change permissions. Do not forget to scan web hosted directories. Access control can be used on these servers to keep them relatively safe. It is also important to scan before backups to protect the restored files from reintroducing viruses.
- Action 7.2.3 Most modern enterprise anti-virus software includes functionality for updating virus definitions and the scanners on workstations. It is important to make use of this functionality to keep up to date on virus definitions.
- Action 7.2.4 Implement mail and gateway scanning.
- ▲ Action 7.2.5 (Advanced) Test all new software on non-networked computers before deploying it on the network.

STEP 7.3.

Check for and remove ROLLBACK.

Problem: *Microsoft inadvertently distributed ROLLBACK.EXE on some Windows NT version 4.0 server and workstation CDs (and possibly on early Resource Kit CDs). When executed, ROLLBACK destroys critical system information including the Registry, user account information, and more. The only fix for this is to restore the entire system from a current tape back up, provided one is available. The Emergency Repair Disk can not restore the system since it requires the SETUP.LOG and Registry components which ROLLBACK.EXE deletes.*

- Action 7.3.1 Check for ROLLBACK.EXE on the hard disk and if it is present, remove it. System users and properties (including those discussed in this booklet) change over time. Many managers consider the following group of activities to be the primary responsibility and value of security professionals. Monitoring all but the smallest installations requires automated tools. Note: SANS has published a booklet comparing user experiences with various third-party NT Security tools.

STEP 8.1.

Regularly monitor and update domain, group, user, and file security status.

Problem: *Without regular monitoring, strong walls begin to crumble.*

- Action 8.1.1 Remove user permissions and remote access immediately upon termination of employment. Some organizations remove users when they announce they will be leaving. This process will be made feasible if the human resources organization establishes a procedure for informing the security staff (automatically) when terminations are effected and/or announced.
- Action 8.1.2 Set contractor accounts to expire periodically (90 - 180 days).
- Action 8.1.3 Establish a regular (no less often than monthly) monitoring program to review security policies and permissions to look for needed changes in: Ownerships, Group memberships—especially Administrator and operator Access permissions, File permissions, Rights and abilities, Trust relationships among domains, and Unknown or unneeded services
- Action 8.1.4 Disable idle user accounts that have not been used for a period of time. One month is typically an appropriate cutoff. If the accounts need to be reinstated this can easily be done.
- Action 8.1.5 Microsoft recommends that you disable accounts for users leaving the organization rather than delete them, so that they can be easily renamed and assigned to a replacement. This is generally not a good idea since users often accumulate privileges over time which may not be directly related to their jobs and it may result in an inadvertent release of information.
- Action 8.1.6 The data owners are responsible for determining appropriate access to their information. In addition, they are usually in the best position to know of employee new hires, terminations, and transfers. To confirm access rights with data owners, prepare a report of access rights for their systems. Submit the report in writing, via hard copy or email, and specifically state that a lack of response indicates approval. After making any necessary changes, file these reports, along with any responses, for your records.

PHASE 8

MONITORING AND UPDATING SECURITY AND RESPONDING TO INCIDENTS

STEP 8.2.

Establish procedures and call lists for responding to incidents.

Problem: *No security wall is impenetrable, so you'll need to be prepared to respond intelligently when an incident occurs. Incident response is a large problem and is the topic of another SANS Step-by-Step booklet. For the purposes of this booklet we offer only two actions:*

- Action 8.2.1 Prepare a call list of people to contact and managers with authority to make key decisions (on whether to shut down or continue operating) and record home, cell, and significant-others' phone numbers, pagers and other contact information for those individuals. Update the list periodically.
- Action 8.2.2 Create, document, and test a recovery procedure.

WINDOWS NT SECURITY

S T E P B Y S T E P

A FINAL WORD

Despite all the good work of careful administrators and well-behaved users, some sites encourage security breaches by assuming all new employees and contracted staff members are honest and stable. If your corporate information assets are valuable, then it makes no sense to give keys to thieves. Conduct detailed background checks on each of your employees and each of your contractors' employees with Administrator privileges. Require bonding of contractor personnel. Establish a contingency plan in case the current Administrators become unavailable or malicious. If the value of the information being protected is very high (as in law enforcement, financial services, or national security) make the checks extend a full five years back into the person's history.

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE O GENERAL SECURITY GUIDELINES

CHECKLIST

STEP		Name of Person Responsible	Date Completed	Initials
STEP 0.1	■ Enforce the least privilege principle.			
STEP 0.2	■ Carefully plan groups and their permissions.			
STEP 0.3	■ Identify the owners of the data files on your systems.			
STEP 0.4	■ Limit trust.			
STEP 0.5	■ Secure RAS.			
STEP 0.6	■ Do not allow modems in workstations unless absolutely necessary.			
STEP 0.7	■ Limit access to Network Monitor.			
STEP 0.8	■ Use third-party authentication.			
STEP 0.9	■ Keep your systems up to date.			

Comments:

WINDOWS NT SECURITY

S T E P B Y S T E P

CHECKLIST

PHASE 1 SETTING UP THE MACHINE

STEP	1.1. Physically secure the server.	Name of Person Responsible	Date Completed	Initials
■ Action 1.1.1	Place the server in a locked room with access controlled by the administrator.			
▲ Action 1.1.2	(Advanced) Provide electronic access control and recording for the server room.			
■ Action 1.1.3	Provide temperature and humidity controls sufficient to avoid damage to the equipment.			
▲ Action 1.1.4	(Advanced) Provide one or more chemical-based automatic fire extinguishers.			
■ Action 1.1.5	Install a UPS (uninterruptible power supply) and associated software.			
▲ Action 1.1.6	(Advanced) Use surveillance cameras to record who accesses the equipment.			
■ Action 1.1.7	Lock the CPU case and set up a system to ensure the key is protected.			
■ Action 1.1.8	Arrange the room so that the keyboard is hidden from view by prying eyes.			
STEP	1.2. Protect the system from undesirable booting.	Name of Person Responsible	Date Completed	Initials
■ Action 1.2.1	Set the "boot sequence" to start with the hard drive "C".			
■ Action 1.2.2	On mission-critical servers disable the floppy drive and CD-ROM.			
■ Action 1.2.3	If the machine is not in a physically secure room, set a BIOS password.			
STEP	1.3. Set up storage protection for back-up tapes.	Name of Person Responsible	Date Completed	Initials
■ Action 1.3.1	Put the back-up tape drive in a secured room.			
■ Action 1.3.2	Set up a secure off-site storage system for back-up tapes.			
■ Action 1.3.3	For short-term storage, place back-up tapes in a locked cabinet.			
■ Action 1.3.4	Ensure that the tape rotation scheme is sufficient to protect the system and meet any legal requirements.			
STEP	1.4. Manage the Page File.	Name of Person Responsible	Date Completed	Initials
■ Action 1.4.1	Set page file size.			
■ Action 1.4.2	Clear page file at system shutdown.			

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 3 SETTING REGISTRY KEYS

CHECKLIST

STEP 3.1.	Manage logon information display and cached logons.	Name of Person Responsible	Date Completed	Initials
■ Action 3.1.1	Disable the display of the last logged on username.			
■ Action 3.1.2	Disable caching of logon information.			
■ Action 3.1.3	Disable automatic logon.			
STEP 3.2.	Use the logon message to warn away intruders.	Name of Person Responsible	Date Completed	Initials
■ Action 3.2.1	Use the logon message to warn uninvited users.			
■ Action 3.2.2	Likewise, set up a login message for FTP users.			
STEP 3.3.	Disable floppy disk drives and hide drive letters.	Name of Person Responsible	Date Completed	Initials
■ Action 3.3.1	Lock access to floppies using Resource Kit service FLOPLOCK.			
■ Action 3.3.2	Disable AutoRun on drives and shares.			
■ Action 3.3.3	On workstations, hide those drives which users do not need to use.			
STEP 3.4.	Enforce strong passwords (Registry portion).	Name of Person Responsible	Date Completed	Initials
■ Action 3.4.1	Install latest Service Pack and modify the Notification Packages value.			
■ Action 3.4.2	A custom password filter can be written and installed if necessary.			
STEP 3.5.	Avoid the Netware DLL Trojan horse.	Name of Person Responsible	Date Completed	Initials
■ Action 3.5.1	Remove the entry FPNWCLNT (the Netware DLL).			
STEP 3.6.	Secure print drivers.	Name of Person Responsible	Date Completed	Initials
■ Action 3.6.1	Add the registry value for HKEY_LOCAL_MACHINE.			
STEP 3.7.	Enable audits of backups and restores.	Name of Person Responsible	Date Completed	Initials
■ Action 3.7.1	Set registry value for HKEY_LOCAL_MACHINE			
STEP 3.8.	Restrict anonymous logon.	Name of Person Responsible	Date Completed	Initials
■ Action 3.8.1	Set another registry value in HKEY_LOCAL_MACHINE			

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 3 SETTING REGISTRY KEYS

CHECKLIST

STEP 3.9. Control remote access to the registry. <ul style="list-style-type: none"> ■ Action 3.9.1 Restrict network access to the registry. 	Name of Person Responsible	Date Completed	Initials
STEP 3.10. Restrict anonymous network access to Registry and other named pipes. <ul style="list-style-type: none"> ■ Action 3.10.1 Use the capability to restrict anonymous (null session) logons. 	Name of Person Responsible	Date Completed	Initials
STEP 3.11. Control access to the command scheduler. <ul style="list-style-type: none"> ■ Action 3.11.1 If server operators need to use the scheduler service, create or assign a registry key value in HKEY_LOCAL_MACHINE ■ Action 3.11.2 Restrict access to the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Schedule to only those users/groups (preferably Administrators only) that are allowed to submit jobs to the schedule service. 	Name of Person Responsible	Date Completed	Initials
STEP 3.12. Secure the Registry. <ul style="list-style-type: none"> ■ Action 3.12.1 Set the ACL entry for the Authenticated Users group to read for those keys to which these users need access. ■ Action 3.12.2 Ensure that the AEDebug key is adequately protected. ■ Action 3.12.3 Secure other registry keys. 	Name of Person Responsible	Date Completed	Initials
STEP 3.13. Block the 8.3 attack. <ul style="list-style-type: none"> ■ Action 3.13.1 Modify part of HKEY_LOCAL_MACHINE. 	Name of Person Responsible	Date Completed	Initials
STEP 3.14. Implement NTLM v.2. <ul style="list-style-type: none"> ■ Action 3.14.1 Modify part of HKEY_LOCAL_MACHINE. 	Name of Person Responsible	Date Completed	Initials
STEP 3.15. Secure NetLogon Channel. <ul style="list-style-type: none"> ■ Action 3.15.1 Modify part of HKEY_LOCAL_MACHINE. 	Name of Person Responsible	Date Completed	Initials
STEP 3.16. Mitigate the Risk of SYN Flood Attacks. <ul style="list-style-type: none"> ■ Action 3.16.1 Modify part of HKEY_LOCAL_MACHINE. 	Name of Person Responsible	Date Completed	Initials

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 4 ESTABLISH STRONG PASSWORD CONTROLS AND SECURE ACCOUNT POLICIES

CHECKLIST

STEP	4.1.	Lockout attempts to gain access after a set number and make passwords hard to guess.	Name of Person Responsible	Date Completed	Initials
■ Action 4.1.1		In the User Manager Properties window, set a password for each new account, enable User Must Change Password at Next Logon, and disable Password Never Expires.			
■ Action 4.1.2		Ensure that all accounts have passwords.			
■ Action 4.1.3		Make passwords hard to guess and force them to change frequently, using the setting listed at 4.1.3 on page 23.			
STEP	4.2.	Enable Administrator account lockout and rename the Administrator account.	Name of Person Responsible	Date Completed	Initials
■ Action 4.2.1		Install the passprop.exe utility included in the NT Resource Kit.			
■ Action 4.2.2		Rename the Administrator account to some other name.			
■ Action 4.2.3		Create a bogus account called Administrator without administrative privileges.			
STEP	4.3.	Establish separate accounts for Administrators.	Name of Person Responsible	Date Completed	Initials
■ Action 4.3.1		Give Administrators separate personal accounts.			
STEP	4.4.	Set up an Administrator password control process.	Name of Person Responsible	Date Completed	Initials
■ Action 4.4.1		Seal the local Administrator password in an envelope and lock it up.			
■ Action 4.4.2		Set the "Password Never Expires" setting for this account.			
■ Action 4.4.3		Use extended ASCII characters in the password for this account.			
STEP	4.5.	Tighten the use of the Everyone group.	Name of Person Responsible	Date Completed	Initials
■ Action 4.5.1		Replace the user "Everyone" with "Authenticated Users".			
■ Action 4.5.2		Disable Guest account.			
STEP	4.6.	Avoid giving Administrator privileges for most tasks.	Name of Person Responsible	Date Completed	Initials
■ Action 4.6.1		Use less privileged accounts when people ask for Administrator privileges.			
■ Action 4.6.2		Avoid Full Control permissions for Everyone (or Authenticated Users) and limit Change access to users who need to delete and/or modify files and directories.			
■ Action 4.6.3		Tighten security on critical files.			

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 4 ESTABLISH STRONG PASSWORD CONTROLS AND SECURE ACCOUNT POLICIES

CHECKLIST

STEP	4.7. Secure and Manage Event Logs.	Name of Person Responsible	Date Completed	Initials
■ Action 4.7.1	Use less privileged accounts when people do not need more privileges.			
■ Action 4.7.2	Copy log files to a different computer.			
■ Action 4.7.3	Set the NTFS permissions on the event log files to allow only Administrators and System access.			
■ Action 4.7.4	Turn on auditing for the event log files.			
STEP	4.8. Avoid using shared accounts—along with an exception.	Name of Person Responsible	Date Completed	Initials
■ Action 4.8.1	Deny requests for shared accounts.			
■ Action 4.8.2	Exception: In a manufacturing environment where shared accounts are absolutely necessary, limit privileges and restrict workstations on which they can be used.			
STEP	4.9. Run an ACL reporting tool.	Name of Person Responsible	Date Completed	Initials
■ Action 4.9.1	Run a third-party reporting tool against both Administrator and user accounts.			
STEP	4.10. Encrypt SAM's password database with 128 bit encryption.	Name of Person Responsible	Date Completed	Initials
■ Action 4.10.1	Enable the feature in Service Pack 3 that allows 128-bit ("strong") encryption of passwords in SAM.			
STEP	4.11. Set appropriate User Rights.	Name of Person Responsible	Date Completed	Initials
■ Action 4.11.1	Set user rights through User Manager for Domains.			

PHASE 5 AUDITING

STEP	5.1. Turn on auditing.	Name of Person Responsible	Date Completed	Initials
■ Action 5.1.1	Turn on event auditing.			
■ Action 5.1.2	Set up file, RAS, printer and Registry auditing as your site policy requires.			
■ Action 5.1.3	Set up logging so that it doesn't over-write the logs as they fill up. (See Step 3.3.)			
■ Action 5.1.4	Save the audit files daily in both event format and in comma-separated-value format.			
▲ Action 5.1.5	(Advanced) Enable CrashOnAuditFail.			

WINDOWS NT SECURITY

S T E P B Y S T E P

CHECKLIST

PHASE 5 AUDITING

STEP 5.2. Monitor the audit logs.	Name of Person Responsible	Date Completed	Initials
■ Action 5.2.1 Set a regular schedule for examining security event logs for failed login attempts.			
■ Action 5.2.2 Use a third-party filtering and analysis tool.			
■ Action 5.2.3 Use centralized monitoring.			

PHASE 6 NETWORKING AND INTERNET SECURITY SETTINGS

STEP 6.1. Turn off all unneeded network services and run needed services safely.	Name of Person Responsible	Date Completed	Initials
■ Action 6.1.1 Turn off all of services not required for servicing remote networked users.			
■ Action 6.1.2 Verify that the services you are running are the latest versions.			
■ Action 6.1.3 Refrain from using domain accounts for services.			
■ Action 6.1.4 Make local accounts with the same name on different machines use different passwords.			
STEP 6.2. If you use Internet Information Server (IIS), block known vulnerabilities.	Name of Person Responsible	Date Completed	Initials
■ Action 6.2.1 Do not install IIS on a domain controller.			
■ Action 6.2.2 Place the Web Server in the DMZ and use the external router to control the Internet traffic.			
■ Action 6.2.3 Do not install a printer on the IIS machine.			
■ Action 6.2.4 Install the web folders on a drive other than the system drive.			
■ Action 6.2.5 Remove IIS sample pages.			
■ Action 6.2.6 Remove the virtual directory \Iisampwd.			
■ Action 6.2.7 Move, rename, or delete any command-line utilities.			
■ Action 6.2.8 Apply the very latest Service Packs and hot fixes.			
■ Action 6.2.9 Disable unnecessary services and features.			
■ Action 6.2.10 Disable .htr mapping if it is not needed.			
■ Action 6.2.11 Remove the Microsoft Data Access Components functionality unless specifically needed.			
■ Action 6.2.12 Secure the anonymous IIS account (IUSR_computername).			

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 6 NETWORKING AND INTERNET SECURITY SETTINGS

CHECKLIST

STEP		Name of Person Responsible	Date Completed	Initials
6.2.	If you use Internet Information Server (IIS), block known vulnerabilities, continued			
■ Action 6.2.13	Ensure that the IUSR_computername account does not have write access to any files on the system.			
■ Action 6.2.14	Disable parent Paths.			
■ Action 6.2.15	Take advantage of IP address restrictions.			
■ Action 6.2.16	Use either Challenge/Response authentication or Basic authentication with SSL encryption.			
■ Action 6.2.17	Do not assign both the Write and Script/Execute permissions to the same folder.			
■ Action 6.2.18	Use the Script permission for Active Server Pages and CGI scripts.			
■ Action 6.2.19	Use NTFS on all IIS hard drives.			
■ Action 6.2.20	Enable W3C Extended logging to keep detailed records of client-server interaction.			
■ Action 6.2.21	Disable directory browsing, especially on folders containing scripts or executable.			
■ Action 6.2.22	Unless absolutely required, uninstall the HTML version of the Internet Service Manager utility.			
■ Action 6.2.23	When using FTP, only allow anonymous access.			
■ Action 6.2.24	Avoid allowing FTP upload or write privileges.			
■ Action 6.2.25	Set a relatively short connection time-out period, and a limited number of simultaneous sessions on FTP servers.			
■ Action 6.2.26	Consider using Virtual Private Networking technologies along with FTP when FTP is necessary.			
■ Action 6.2.27	If at all possible, do not install the Microsoft FrontPage Server Extensions and do not allow users to manage their personal web sites with FrontPage.			
■ Action 6.2.28	Do not install Microsoft Index Server if it will not be used.			
■ Action 6.2.29	If you wrote your own web applications, it is crucial to always perform proper bounds checking and validation of input data.			
6.3.	Protect vulnerable ports through a firewall (or screening router).			
■ Action 6.3.1	Block ports 135 (RPC), 137 (nbname), 138 (nbdatagram) and 139 (nbssession).			
■ Action 6.3.2	Install the latest Service Packs relevant to your installation.			

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 7 OTHER ACTIONS REQUIRED AS THE SYSTEM IS SET UP

CHECKLIST

STEP		Name of Person Responsible	Date Completed	Initials
STEP 7.1.	Require password-protected screen savers on all workstations.			
■ Action 7.1.1	Provide all users with password protected screen savers.			
■ Action 7.1.2	Teach users to press Ctrl-Alt-Del and then "Lock Workstation" whenever they leave.			
STEP 7.2.	Implement virus protection software.			
■ Action 7.2.1	Install on-access virus scanning software on all workstations. Install software that searches for and eradicates viruses on all servers. Set a regular scanning schedule, or use on-access scanning. Note, however, that on-access scanning can be resource intensive and a trade-off may need to be made between security and availability.			
■ Action 7.2.2	On heavily-used servers, where on-access and/or full scanning is too resource intensive, concentrate scans on sensitive areas. These include user directories, and anywhere else where users have Full Control or Change permissions. Do not forget to scan web hosted directories. Access control can be used on these servers to keep them relatively safe. It is also important to scan before backups to protect the restored files from reintroducing viruses.			
■ Action 7.2.3	Use your anti-virus software's ability to update virus definitions and scanners on workstations. Do this regularly to keep up to date.			
■ Action 7.2.4	Implement mail and gateway scanning.			
▲ Action 7.2.5	(Advanced) Test all new software on non-networked computers before deploying it on the network.			
STEP 7.3.	Check for and remove ROLLBACK.	Name of Person Responsible	Date Completed	Initials
■ Action 7.3.1	Check for ROLLBACK.EXE on the hard disk and if it is present, remove it.			

Comments:

WINDOWS NT SECURITY

S T E P B Y S T E P

PHASE 8 MONITORING AND UPDATING SECURITY AND RESPONDING TO INCIDENTS

CHECKLIST

STEP	8.1. Regularly monitor and update domain, group, user, and file security status.	Name of Person Responsible	Date Completed	Initials
■ Action 8.1.1	Remove user permissions immediately upon termination of employment.			
■ Action 8.1.2	Set contractor accounts to expire periodically (90 - 180 days).			
■ Action 8.1.3	Establish a regular (no less often than monthly) monitoring program.			
■ Action 8.1.4	Disable idle user accounts which have not been used for a period of time. One month is typically an appropriate cutoff. If the accounts need to be restored to use this can easily be done.			
■ Action 8.1.5	Microsoft recommends that you disable accounts for users leaving the organization rather than delete them, so that they can be easily renamed and assigned to a replacement. This is generally not a good idea since users often accumulate privileges over time which may not be directly related to their jobs, and it may result in an inadvertent release of information.			
■ Action 8.1.6	Confirm access rights with data owners. Repeat this periodically.			
STEP	8.2. Establish procedures and call lists for responding to incidents.	Name of Person Responsible	Date Completed	Initials
■ Action 8.2.1	Prepare a call list of people to contact and managers with authority to make key decisions.			
■ Action 8.2.2	Create, document, and test a recovery procedure.			

FINAL STEP

FINAL STEP	Perform background checks on all persons with Administrator privileges.	Name of Person Responsible	Date Completed	Initials

Comments:

APPENDIX: USEFUL RESOURCES FOR NT SECURITY PROFESSIONALS

WEB SITES ON WINDOWS NT SECURITY

The web sites that our contributors most often watch:

<http://www.microsoft.com/security>
<http://www.cert.org/>
<http://ciac.llnl.gov/ciac/>
<http://www.ntsecurity.net/>
<http://www.l0pht.com>
<http://www.sysinternals.com/>
<http://www.ntbugtraq.com>
<http://www.it.kth.se/~rom/ntsec.html>
<http://www.foundstone.com>
(Formerly NT OBJECTives, Inc.)
<http://www.securityfocus.com>
<http://www.securiteam.com>
<http://packetstorm.securify.com>
<http://razor.bindview.com>

ADVANCED TRAINING PROGRAMS FOR WINDOWS NT AND WINDOWS 2000 SECURITY

The SANS Institute has established an intensive immersion curriculum for administrators and security professionals who need advanced expertise in securing Windows systems. Both classroom and online training programs are available. See <http://www.sans.org> for details on both types of programs.

ABOUT THE SANS INSTITUTE

The SANS Institute is a cooperative research and education organization through which system administrators, security professionals, and network administrators share the lessons they are learning. It offers educational conferences and in-depth courses, cooperative research reports, and electronic digests of authoritative answers to current questions.

Microsoft's official hotfix and service release site is at <http://support.microsoft.com/support/ntserver/hotfixes.asp>. However, this site is sometimes not completely up to date.

You should monitor the official FTP site for hotfixes at: [ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/ <your 3-letter language code>/nt40/hotfixes-post<your service pack level>/](ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/<your 3-letter language code>/nt40/hotfixes-post<your service pack level>/).

For example, the FTP site for the US versions of post service pack 4 hotfixes is:

<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP4/>

Microsoft's knowledge base, which contains all technical support articles, is available online at <http://support.microsoft.com/support/c.asp>

Microsoft also publishes the entire knowledge base as part of TechNet. TechNet is an invaluable source of information that should not be missing in any administrator's toolkit. For more information see <http://www.microsoft.com/technet/default.htm>

Microsoft now has a security email list where they announce new issues. To subscribe send email to microsoft_security-subscribe-request@announce.microsoft.com with subscribe as the message text.

In addition, the vast majority of the contributors subscribe to the Security Alert Consensus and the Windows Security Digest which provide definitive weekly and monthly summaries of new threats and actions needed to counter the threats. The digests serve as time savers for administrators who cannot monitor all the web sites.

Subscribe to the Security Alert Consensus by emailing info@sans.org with subject SAC.

Subscribe to the Windows security Digest by emailing info@sans.org with subject Windows Security Digest.

WINDOWS **NT**
SECURITY
STEP BY STEP
THE SANS INSTITUTE

Copyright 2001. The SANS Institute. No copying or forwarding allowed except with written permission.