the CENTER for
INTERNET SECURITY

Level One Benchmark
Windows NT 4.0 Operating Systems
V1.0.5

Terms of Use Agreement

Background.

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

No representations, warranties and covenants.

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

User agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**we**") agree and acknowledge that:

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

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

Grant of limited rights.

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

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

Retention of intellectual property rights; limitations on distribution.

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

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

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

Special rules.

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

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

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

Choice of law; jurisdiction; venue.

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

We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

V1.0.5 Benchmark
August 28, 2003

This document is a first generation Level I Benchmark for the Microsoft Windows NT 4.0 operating system. It is a combination of best practices published by The SANS Institute, the security community, and advice from members of the Center for Internet Security (CIS).

CIS Level I Benchmarks define minimum standards for securing various operating systems including Windows, and variations of Unix. These standards should be used to improve the "out of the box" security of common operating system software to a prudent "due care" minimum level. By definition, the security actions included in CIS Level I Benchmarks satisfy three conditions: (1) they can be safely implemented by a system administrator of any level of technical security skill, (2) they will generally "do no harm" to functionality commonly required by everyday users, and (3) they can be scored by an associated software tool. This document is an example of a Level I Benchmark.

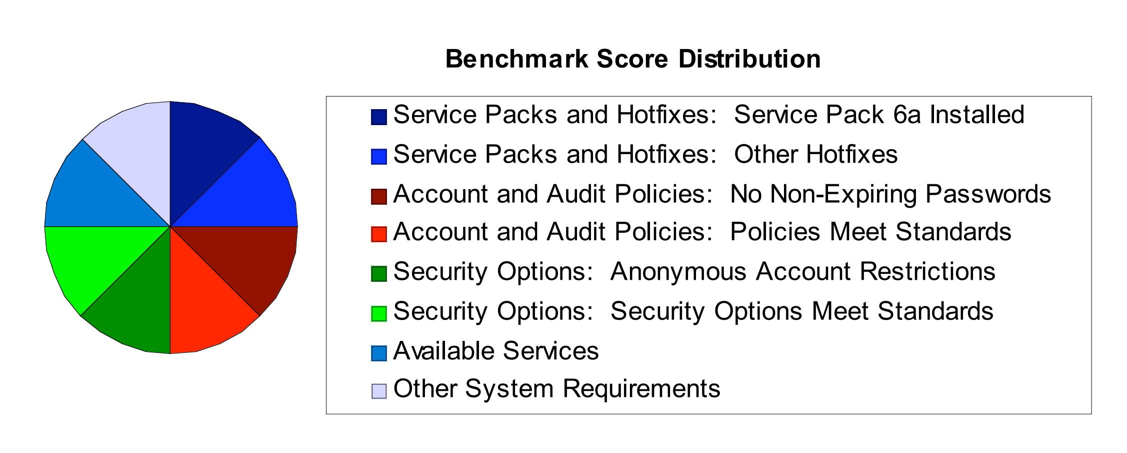
Level II Benchmarks are more detailed, and more specialized with regard to specific applications or functions running on an operating system platform. These standards may recommend or require that certain functionality be restricted in light of the associated risk. Examples of Level II Benchmarks include Internet Information Services, Terminal Services, or Microsoft SQL Server. Creating Level II Benchmarks often involves joint effort by specialists in both application and operating system security.

Keeping Score

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

The criteria used for scoring are divided into four categories: (1) Service Packs and Hotfixes, (2) Policies, and (3) Security Settings - each receiving one-quarter (or 2.5 out of 10) of the score, and (4) Available Services and Other System Requirements accounting for the final quarter of the score. Additional applications, or Services, may detract from the overall score, just as additional services detract from the security of these systems in the production environment. Level II Benchmarks may cover such Services in the future.

Each of these three primary categories has a limited number of *major requirements* and many *minor requirements*. For example, in the area of Service Packs and Hotfixes, the current Service Pack is a major requirement, while other Hotfixes may be considered minor. The major and minor elements of each category are discussed in the following sections.



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

Intended Audience

This benchmark is intended for anyone using a Windows NT 4.0 operating system who feels at all responsible for the security of that system. A Security Manager or Information Security Officer should certainly be able to use this guide and the associated tools to gather information about the security status of a network of Windows NT 4.0 computers. The owner of a Small Office/Home Office can use this guide as a straightforward aid in enhancing his or her own personal network security. A Windows System Administrator can use this guide and the associated tools to produce explicit scores that can be given to management to reflect where they currently stand, versus where they should stand with regard to security.

Any user who uses this guide to make even the slightest improvement on the secure state of a system might be doing just enough to turn a potential hacker or cracker away to an easier target. If enough people become "Security Aware Users" then the safety level of the Internet will have improved dramatically.

Practical Application

Just as there is often no single correct way to get to a specific destination, there is more than one way to implement the settings and suggestions described in this text. In a network environment, with a Windows NT 4.0 Domain, Group Policy can be used to apply nearly all the settings described herein. Many surveys of Fortune 500 or Fortune 1000 companies have indicated that large companies have hesitated to migrate to Windows 2000 Active Directory because of the level of complexity involved. Many of these settings can be implemented through Windows NT 4.0 or Windows 2000 domain Group Policy. The examples given in this text will be implemented as recommended by Microsoft, by directly editing the registry.

A method involving the use of the Microsoft Security Configuration and Analysis Utility, to automatically install the template (cis.inf) which includes the security settings contained in this benchmark, is described in documentation that accompanies the scoring tool.

Updates, Bug-Fixes, and Enhancements

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

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

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

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

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

Major Service Pack and Hotfix Requirements:

Microsoft originally intended to release Service Packs for its Windows NT based operating systems as often as once each quarter. This goal has proven to be logistically infeasible, and Service Packs are currently released as necessary. The current service pack available for Windows NT 4.0 is Service Pack 6a, and Microsoft has decided not to release any further service packs. Additional updates will be released as Hotfix Roll-ups.

Microsoft has historically required that computers be updated to the current Service Pack before offering detailed technical support. A link to obtain the current Service Pack is available in Appendix A.

Minor Service Pack and Hotfix Requirements:

Hotfixes are not released on a schedule. They are produced as new bugs and vulnerabilities are discovered. As a result, publishing a list of Hotfixes is only valid as of the date of the publication. There is a link to the available Hotfixes for Windows NT 4.0 below.

The process of discovering which hotfixes are needed has been automated since the release of Windows 2000. Windows NT 4.0 enjoys this same benefit thanks to the release of Internet Explorer 5 and above. Open Internet Explorer, click the Tools drop-down menu, and click “Windows Update”. Click the link to Product Updates. When asked if you trust Microsoft, say yes to proceed. Windows update will take a few moments and analyze your system, and identify the Critical Updates and Service Packs, Advanced Security Updates, Recommended Updates, and Device Driver updates which are available.

The Critical Updates and Service Packs, and Advanced Security Updates must be installed for the score of this benchmark. Some updates must be installed individually, while others may be installed concurrently before a reboot is required. Some of these updates are rather large, and should be installed over a high-speed connection if available.

A current list of patches is available from Microsoft’s web site at the following Internet Address: http://www.microsoft.com/ntserver/nts/downloads/default.asp.

Auditing and Account Policies

While many system attacks take advantage of software inadequacies, many also make use of user accounts on a Windows computer. In order to prevent this sort of vulnerability, "policies" or rules define what sort of account/password "behavior" is appropriate, and what auditing behavior is required. The configuration of user account policies is inadequate or disabled in a default installation.

Account Policies answer questions like "How often do I need to change my password?" or "How long or how complex does my password need to be?" These policies are often left disabled or weak, leaving many machines vulnerable to attack with little or no effort.

Auditing Policies determine what sorts of security transactions are recorded in the Security Event Log. By default, nothing is retained in the Security Event Log, so any attempts to compromise a system go completely unrecorded. Logging events is crucial for analysis in the aftermath of an intrusion incident.

Major Auditing and Account Policies

There are so many important account policies, that it is difficult to pin down what the "worst offender" is, with regard to how accounts are handled. Password length and complexity are obviously important, but so is another factor that extends beyond a written policy: When accounts are created or maintained, they are often set to have passwords that never expire – overriding the accepted account policy.

The major account-related policies should be split between two factors:

- Minimum Password Length of 8 characters.
- All account passwords are no more than 90 days old.

There are arguments to be made that passwords of more than 7 characters are no more difficult to crack than passwords of exactly seven characters.

Administrators are occasionally required to assign administrative accounts to services requiring extraordinary rights. In doing so, it becomes a time consuming process to change these passwords, especially across an enterprise. Just like changing the passwords of administrative "user" accounts, these administrative "service" accounts need to have their passwords changed on a regular basis.

Minor Auditing and Account Policies

Audit Policy

An Audit Policy determines what facts, or events, an individual system should remember or record. This is often the only record that a password attack has been attempted.

These events are not retained at all unless a computer is specifically configured to do so. This audit policy can record Success or Failure events within defined categories. The following types of events should be logged:

Audit Policy	
Logon and Logoff	Success, Failure
File and Object Access	Failure
Use of User Rights	Failure
User and Group Management	Success, Failure
Security Policy Changes	Success, Failure
Restart, Shutdown, and System	Success, Failure
Process Tracking	None

Two types of audit events can be logged: Success and Failure. In most cases, both types of events are important.

Logon and Logoff

The most basic event to record is an Account Logon event. Auditing failed logons can alert administrators to attempted logon compromises, and auditing successful logons can track users who have logged on to the system. These successful logons should be compared against known access times to see if accounts have been compromised.

File and Object Access

Object Access is often one of the most misunderstood auditing categories on Microsoft operating systems. The common misconception is that if both success and failure events are recorded, the event logs will fill up immediately because it logs all access to all files. This is not the case.

If object access auditing is enabled, then the event log is ABLE to log access events ONLY if logging has been configured for a specific user on specific objects – usually files or folders. If those objects are configured to audit access of either success or failure, but the Audit Policy does not support the corresponding event type, no audit logging will occur.

Use of User Rights

Many of the abilities that make up “Administrator” access can be broken down into User Rights. These rights can be assigned to non-administrative accounts enabling them to perform actions on the operating system with more privileges than would be possible if they were a “normal” user account. While the successful use of these rights is commonplace, failed use of these rights should be recorded in the event log to identify when accounts are attempting to use these rights.

User and Group Management

Account Management auditing records information such as account creation, deletion, or modification of account attributes, passwords, and user rights. Success and Failure events should be logged.

Security Policy Changes

Changes to user rights, security options, or audit policies are recorded if auditing of Policy Changes is enabled. If this is not enabled, no record of those changes is retained.

Restart, Shutdown, and System

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

Process Tracking

Each time a process is created, paused, stopped, or destroyed, an event can be generated in the Security Event Log. This option should only be enabled as an aid to application development, or in an effort to track down virus activity. In most cases, it can remain disabled for success and failure auditing.

Account Policy

A list of minimum acceptable account policies is attached below, along with a description of what each policy means.

Password Policy:	
Maximum Password Age	90 Days
Minimum Password Age	1 Day
Minimum Password Length	8 Characters
Password Uniqueness	24 Remembered
Account Lockout Policy	
Lockout after:	5 Bad Login Attempts
Reset count after:	60 Minutes
Lockout Duration:	60 Minutes
Password Complexity	Enabled

Maximum Password Age

In order to ensure that users change passwords on a regular basis, policy must determine how long accounts are permitted to use the same password. If this is set to zero, passwords will never expire. This setting can otherwise be set up to 998 days. Any setting of 90 days or less should be deemed acceptable.

Minimum Password Age

The purpose for requiring a minimum password age is to prevent users from using their favorite password until it expires, and changing their password more times than the system remembers, and cycling back to their favorite password, thus circumventing the system. Set the Minimum Password Age to at least one day.

Minimum Password Length

The length of a password is one factor that determines the difficulty and time required to “crack” it. The NSA requires passwords of at least 12 characters. It is uncommon for most business systems to require passwords of that length. The generally accepted standards vary between 7 or 8 character passwords. In conjunction with sufficient complexity, a 7 character minimum password length becomes difficult enough to guess or crack by “brute force” in its useful lifetime.

Password Uniqueness

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

Account Lockout Policy

One method of gaining access to a computer system is to keep trying to access that system from the network, using common account names, and different passwords until one works. Dictionary attacks use lists of common words as passwords in attempts to logon to a system. They are often successful against weak passwords. Brute Force attacks attempt to use every possible character combination as a password, and will always be successful given enough time.

In order to combat these attacks, an Account Lockout Policy will disable an account after a specified number of failed logins occurs during a defined period of time. That account will remain locked out for a defined period of time. Enabling lockout policies make these attacks mathematically infeasible.

Lockout Account After 5 Bad Login Attempts

How many failed logons for a specific account is too many? If users get their passwords wrong too many times, they will effectively lock themselves out of their own account. This threshold should be set to no more than 5 failed logons.

Reset Count After 60 Minutes

The period of time required to lock out an account should be set to 60 minutes. This time period determines how long after the first failed logon it should keep counting the failed logons until it reaches the lockout threshold.

Lockout Duration: 60 minutes

The account lockout duration determines the amount of time that an account remains locked out once the number of failed logons has been reached. This should be set to at least 60 minutes.

Passwords must meet complexity requirements

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

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

An 8 character password made up of only lowercase characters has 8^{26} possible passwords. A 8 character password made up of uppercase, lowercase, and special characters (on a standard 104 key keyboard) has 95 possible keys (excluding control characters) that make for 8^{95} possible password combinations. That's nearly the "simple" set of passwords to the power of four!

How to Enable Auditing Policies

In order to enable Auditing Policies on the local computer, click “Start”, go to “Programs”, then “Administrative Tools”, and open the “User Manager” or “User Manager for Domains” as appropriate. If you are logged in using a local account, User Manager will display a list of accounts from the local machine. If you are logged in using a domain account, click the “File” drop-down menu, and click “Select Domain”. Then type “\\” followed by the name of the local machine, and press “Enter”.

Click the “Policies” drop-down menu, and click “Audit…” Click the appropriate button to enable auditing. Then check the “Success” or “Failure” box next to the appropriate policies for each one you wish to enable.

How to Enable Account Policies

Much like enabling Auditing Policies, open the User Manager or User Manager for Domains. Click the “Policies” drop-down menu, and click “Account…” The next menu will show each of the settings described in the Account Policies and Account Lockout sections of this benchmark.

How to Require Complex Passwords

Requiring complex passwords under Windows NT 4.0 is not integrated into the operating system. There are several ways to accomplish this task, but the easiest way is to get the “passprop.exe” utility from the Windows NT 4.0 Workstation or Server Resource Kit. Run “passprop.exe” while logged in using a local machine account with Administrative rights.

Running PassProp by itself will display the current settings. The command “passprop /complex” will require all accounts to have complex passwords. One other important feature of PassProp is that it can also be used to enable Administrator account lockout with the command “passprop /adminlockout”.

One important note is that the tools available to require complex passwords under Windows NT 4.0 only require them when changing passwords through the standard “user” methods (Press CTRL+ALT+DEL, click Change Password, and so on…) They do not prevent administrators from creating simple passwords using User Manager or User Manager for Domains. Administrative or Account Operator rights CAN be used to circumvent these complex passwords. It is also worth noting that this has been fixed in Windows 2000.

How to check the Security Event Log

Enabling audit policies doesn’t do much good if they are never checked. Make a point of periodically checking the Security Event Log to see what sorts of things are happening in the local network environment. Open Administrative Tools and click “Event Viewer”. The Event Viewer will display all events that have been recorded and are still being retained.

Security Settings

Making security related changes to the various versions of Windows NT often requires the ability to directly edit the registry. This can be a hazardous process, which is not too difficult to do properly, but has the potential to cause catastrophic damage to a system if done improperly. It requires Administrative access, and can be done using the REGEDIT or REGEDT32 command.

Before making any changes to a Windows NT system registry, run the "RDISK" utility, to make an Emergency Repair Disk. This will back up a subset of the registry to a floppy disk, and will help protect a system in the event of registry corruption or mistakes made while editing the registry. Use the command "rdisk /s" to back up the registry and security account information.

Major Security Settings

When Microsoft made the transition from Windows 3.0 and 3.1 to Window 95 and Windows NT, many of the early networking programs used a "Null User" account to transfer data from one machine to another. A Null User is a zero length username with a zero length password. By default, it is still enabled on Windows NT machines today. This user does not have elevated rights on these computers, but it is considered an authenticated user, and still has the ability to gain information that would be valuable in the hands of an attacker.

In order to restrict Null User from listing account information, run REGEDIT. Navigate the Explorer-like interface to HKEY_LOCAL_MACHINE – SYSTEM – CurrentControlSet – Control – LSA and edit the value RestrictAnonymous which should be of type REG_DWORD and have a value of 1.

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

Minor Security Settings

Allow System to be Shut Down Without Having to Log On

By default, Windows NT Workstation enables this option, and Windows NT Server disables it. Whether or not this option should be changed on a computer is entirely subject to its environment. Workstations should probably keep their default settings. Servers may need to keep their default settings as well.

If a server is in a guarded Data Center, it will need rebooted periodically. In some cases, it may be more prudent to allow the server to be rebooted from the console without logging in, as opposed to giving data center operators rights to the machines themselves.

This setting does not apply to benchmark scoring, but judgment must be applied and documented in individual security policies.

It may be changed in REGEDIT by navigating to HKEY_LOCAL_MACHINE – Software – Microsoft – Windows NT – CurrentVersion - Winlogon and editing the ShutDownWithoutLogon value. Set this to 0 to not allow the system to be shut down without logging on, or 1 to allow it.

Disable Automatic Logon

One of the strengths of Windows security is that it requires the CTRL+ALT+DEL key sequence to log on to a computer. It is possible to allow automatic logon of a Windows NT Workstation or Server by saving the logon information in the registry. Aside from the fact that anyone who has access to the console would have valid user access without presenting any credentials, the system is at risk since the user logon information is stored in the registry in plaintext!

In REGEDIT, go to HKEY_LOCAL_MACHINE – Software – Microsoft – Windows NT – CurrentVersion – Winlogon and make sure that the values DefaultDomainName, DefaultUserName, and DefaultPassword either do not exist, or are blank.

LAN Manager Authentication Level

There are three types of network communication involved in Windows NT authentication: Lan Manager (or LM), NT Lan Manager (or NTLM), and NTLM v2. LM communication is the easiest to crack because of the way it is stored. NTLMv2 is the hardest to crack because it was developed from lessons learned over time, and uses better cryptography. Unfortunately, either (or both) of these types of network communication are passed to a client in response to network requests.

Note that requiring NTLMv2 authentication will disable communication with Windows 95/98/Me computers unless they are patched with the DSClient.exe utility that ships with Windows 2000.

Navigate REGEDIT to HKEY_LOCAL_MACHINE – System – CurrentControlSet – Control – LSA and change the value of LMCompadibilityLevel to at least 2, but as applicable below:

0 – Send LM and NTLM response to all network requests – default setting.
1 – Use NTLMv2 Security if negotiated.
2 – Send NTLM authentication only.
3 – Send NTLMv2 Authentication only.
4 – Domain Controller refuses LM authentication.
5 – Domain Controller accepts only NTLMv2 authentication.

Message Text for Users Attempting to Log On

There have been court cases where system intruders have eluded conviction by claiming they were never “warned” not to access a system which is private property. In response, Microsoft has enabled a log-on notice (and the corresponding logon title, next) to allow system administrators to display a legal notice prior to users logging on.

The warning banner should vary from one organization to another, and should not be implemented without legal counsel. Here is a sample message, which should give users an idea of what to expect: "This system is for the use of authorized users only. Individuals using this computer system with authority, without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials." This text has been taken from CERT Advisory CA-1992-19 as quoted from http://www.sans.org/infosecFAQ/incident/evidence.htm.

To enable a logon message, make the following changes to the Windows NT registry under the following key: HKEY_LOCAL_MACHINE – Software – Microsoft – Windows NT – CurrentVersion – Winlogon

LegalNoticeCaption (REG_SZ) "Restricted Computer System"
LegalNoticeText (REG_SZ) "*custom security warning*"

Prevent Users from Installing Printer Drivers

It is feasible for "Trojan Horse" types of programs to be disguised as printer drivers, which seem to be necessary for users to print, but actually do something else malicious. If only administrators are able to install printer drivers, there is no fear that the users can compromise their computers by installing unreliable drivers.

Find the HKEY_LOCAL_MACHINE – System – CurrentControlSet – Control – Print – Providers – LanMan Print Services – Servers in REGEDIT and change the AddPrintDrivers value to 1.

Rename Administrator Account

In order to gain access to a computer system, a prospective user needs a user account and a password. The default name of a valid account on every Windows computer is "Administrator". Hackers know this, and it is one of the things they try. As a matter of policy, this account should be renamed – to anything other than Administrator. The choice of account names should vary from location to location, so long has it has been changed.

Open User Manager and highlight the Administrator account. Click the "User" drop-down menu, and click Rename. Type a new name for the Administrator account, and click OK. Be careful to record exactly what the new account name is. It is also generally a good idea to create an updated Emergency Repair Disk (RDISK /s) after making major account changes like this.

Please be aware that this is not a "silver bullet" against finding the Administrator account. Experienced hackers who have already found a foothold in a local network will eventually be able to discover the account name given enough time. However this CAN help defend against "scripted" attacks.

Take care when renaming the Administrator account. Some applications, enterprise management systems in particular, can be "broken" when this account is renamed, even though those applications don't actually authenticate against this account. Test this setting extensively before implementing it in large numbers.

Rename Guest Account

Just like the Administrator account above, rename the Guest account to something less obvious. This will not be an issue as long as the Guest account remains disabled, but it’s a good idea to change it anyway.

Restrict CD-ROM Access to Locally Logged-On User Only

It is potentially possible for a CD-ROM to be shared like any other part of a Windows file system. Enable this option to prevent users from sharing the local CD-ROM Drive.

Navigate REGEDIT to HKEY_LOCAL_MACHINE – Software – Microsoft – Windows NT – CurrentVersion - Winlogon and set the value of AllocateCDRoms to 1.

Restrict Floppy Access to Locally Logged-On User Only

As with the above setting, Enable this option to restrict access to the local floppy drive to the local user only.

Navigate REGEDIT to HKEY_LOCAL_MACHINE – Software – Microsoft – Windows NT – CurrentVersion - Winlogon and set the value of AllocateFloppies to 1.

Available Services

Each and every computer that responds to network requests has an application or service that answers requests on that network. The more types of network requests that have services answering them, the more potential portals exist for attack. If a service is not being used, it should be disabled or removed. If it is to be used, it should be properly secured and maintained. To determine which services you have running on your system, and to disable any unneeded services, click Start, Settings, Control Panel, and double-click Services.

Securing these applications running on Windows NT 4.0 computers as Services, such as Internet Information Server, DNS Server, SQL Server, and hundreds of others, is beyond the scope of this, or any Level I Benchmark. The Center for Internet Security will be developing Level II Benchmarks as quickly as possible in response to the demands of the Internet community.

Check the CIS web site (http://www.cisecurity.org) to see what other benchmarks are available or in development. CIS Members can also voice an opinion on application benchmark development.

Service Status

To view the list of services installed on any given computer, log on to the console. Click 'Start' -> 'Settings' -> 'Control Panel' and double-click the 'Services' applet. Double-click individual services to make changes to their configuration.

The normal status of a service is 'Started' or 'Stopped'. In addition, services can be 'Paused', 'Starting' or 'Stopping'. If a service status is blank, it is stopped.

It is also useful to note the "Startup Type" of a service. 'Automatic' services start when the computer reboots. 'Manual' services can be started by users or other services, but are not started automatically. Services can also be 'Disabled' and will not start. The Startup Type can be changed, but that requires more permissions than just starting or stopping the services.

Service Permissions

Like so many other things in an operating system, services have permissions tied to them. These permissions are difficult to find and set, but they can be changed. And like so many things in the Microsoft operating systems, these permissions are open to "everyone" with full access by default.

The services on the following page should be configured to allow 'Administrators' to have Full control over them, and grant 'System' the 'Read' and 'Start, Stop, and Pause' permissions. Other permissions on these services should be removed.

The Security Templates Snap-In for the Microsoft Management Console can be used to create custom security templates or to apply settings in an established template. Beware that when settings are applied, they are done so immediately, and there is no "undo" button. Take great care when applying security templates. For more information on how the Security Configuration and Analysis tool can be used to view and set service permissions, see the CIS Windows Implementation Guide accompanying the CIS Windows Security Benchmark Tool.

Warning: Disabling services without understanding what each of them do can make a system unstable or entirely unusable! Not all services are optional. Be careful which services you change.

It is also important to note that some of these services perform functions that users have become accustomed to. When disabling these services, disable one or two at a time, and restart the computer. If you have not lost any functionality, and are comfortable with these changes, move on to the remaining services. In some cases, these services are necessary for some environments. Testing may be required to get a balance between security and functionality.

Alerter

The Alerter service makes it possible for Windows NT computers to "alert" each other of problems. This feature goes largely unused in most circumstances. Disable the Alerter service.

Clipbook

The Clipbook service is used to transfer clipboard information from one computer to another. It is also rarely utilized in Windows NT. Disable the Clipbook service.

Messenger

The Messenger service works in conjunction with the Alerter service. Disable the Messenger service.

Telnet

The Telnet service is not installed in Windows NT by default. If it is installed, it allows a remote user to connect to a machine using a command prompt. It still requires authentication, but does not offer any encryption or security. Disable or remove the Telnet service. If there is a legitimate need for a remote DOS console on a Windows machine, investigate third-part Secure Shell (SSH) utilities instead.

Additional Services

Services run on a computer to perform a function. It is important to know that each service running on any Windows computer has the ability to make use of system resources – processor, memory, disk usage, and so on. One of those resources is the ability to communicate over a network, or the Internet.

No system security plan can be effective unless the active services are defined and action is taken to harden, and/or disable those services. Most applications that run on a computer run as services, and provide a desired functionality. If they are not properly maintained, they may also act as a window of access for an unwelcome guest, regardless of the score generated on a Level 1 Benchmark.

It is not possible to list all of the services that can be installed on a Windows NT computer. The "standard" services that are normally found on a Windows computer are listed below. These services are not all as "secure" as they should be, but they are not restricted, either because doing so would "break" common functions, or because the skill level required is beyond what would be expected for a Level 1 Benchmark.

The assessment tool provided by CIS lists the services currently installed on your machine as it executes, and identifies services outside the list below. These may or may not present a security risk. Take the time to compare these two lists, and find what services may be making your machine vulnerable.

Alerter
Clipbook Server
COM+ Event System
Computer Browser
DHCP Client
Directory Replicator
Event Log
License Logging Service
Messenger
Net Logon
Network DDE
Network DDE DSDM
NT LM Security Support Provider
Plug and Play
Protected Storage
Remote Procedure Call (RPC) Locator
Remote Procedure Call (RPC) Service
Server
SNMP
SNMP Trap Service
Spooler
System Event Notification
Task Scheduler
TCP/IP NetBIOS Helper
Telephony Service
UPS
Windows Installer
Windows Management Instrumentation
Workstation

It is important to know that even if a machine scores a perfect 10 on a Level 1 Benchmark, an improperly configured service can present a vulnerability that bypasses ALL other system security. There are a large number of vulnerabilities to Internet Information Services that emphasize this fact. Other services can be just as vulnerable. **You are advised to contact software manufacturers for security information on other services installed on your system. Due to the vast number of services that may be installed on your system, we are unable to address them all here.**

The Center for Internet Security is committed to addressing these vulnerabilities. As time and resources allow, we will develop Level 2 Benchmarks to address many of these applications. The CIS members have the greatest input on which benchmark standards are addressed in which order. We are continually reviewing and revising existing benchmarks, as well as developing new ones based on feedback we receive.

Other System Requirements

Windows has been innovative, easy to use, and generally flexible. It has not been easy to secure. The preceding chapters represent many of the centrally-located improvements in Windows based security.

While Windows has shown great improvement in the overall security process, there is still no "one source" to answer all security concerns of a system. Some of these settings or actions fall into the "other" category. Many of those security requirements are described below.

Ensure All Disk Volumes Are Using the NTFS File System

Warning: Do not do this if your system is a dual-boot system with Windows 95/98/Me – that is if you have the option of booting into Windows NT or Windows 9x. The alternate operating system will cease to function, and can not be recovered.

Since the early days of DOS, files have been stored on floppy disks. These disks break up data into blocks, and those blocks are written to similar blocks on a physical disk. The "map" describing which blocks are holding which files is stored on part of the disk called the "File Allocation Table" or FAT. When DOS moved to Hard Disks, the same FAT style of disk allocation was used. FAT filesystems had some good points – most of all, it's pretty simple. Any system could read the disks, and if there was a problem, the data could have been restored. When disks began to grow beyond the size of FAT's capabilities, it was expanded to FAT32, allowing for larger disks. However, FAT and FAT32 do not offer any security.

Along came Windows NT, which allowed the user to stick with the FAT hard disks, or use NTFS (NT File System) disks. NTFS offered the ability to assign permissions, or rights, to files and folders that could permit or deny access to those objects. In order for system administrators to use NTFS, they had to abandon FAT completely, which meant they gave up the "ease of use" and general interoperability that accompanied it. As a result, some implementations still use the FAT filesystem.

NTFS interoperability has come a long way since its initial introduction. It can be bypassed if the system can be rebooted, but it is the ONLY way that any file-level security can be enforced while system is operating.

To determine if a disk volume is NTFS, double click "My Computer" on the desktop. Right-click the C drive (C:) and click Properties. The properties pane for that disk will describe the "File System" as either FAT or NTFS.

In order to make a FAT disk into an NTFS disk, open a Command Prompt (Click Start -> Programs -> Accessories -> Command Prompt) and type "Convert C: /fs:ntfs". The system will probably be required to restart to perform this task. Take the same action with the D: drive and any others that show up as FAT disks.

Once a disk is converted from FAT to NTFS, the permissions on that drive need to be fixed. To apply the default security settings to the hard drive, execute FIXACLS.EXE from the Windows NT 4.0 Resource Kit to apply the correct file security.

Other applications will have the ability to use these security features. Most users never need to update these file permissions, while system administrators of all levels will need to do so from time to time. In fact, it is possible to cripple a system by incorrectly modifying that security. It is important to keep in mind that this is still a step up from a FAT filesystem with NO security.

Appendix A: Internet Resources

The Center for Internet Security – http://www.cisecurity.org
The SANS Institute – http://www.sans.org
Microsoft Windows Security – http://www.microsoft.com/security
Current Critical Service Packs and Hotfixes - http://www.microsoft.com/ntserver/nts/downloads/default.asp
Microsoft Directory Services Client for Windows 9x/Me - http://www.microsoft.com/TechNet/prodtechnol/ntwrkstn/downloads/utils/dsclient.asp?frame=true
The CIS Scoring Tool that accompanies this document uses the Microsoft Network Security Hotfix Checker (HfNetChk), which is licensed to Microsoft by Shavlik Technologies – http://www.shavlik.com/

Appendix B: User Rights Assignment

Windows computers reference which users or accounts have rights to perform specific functions by modifying User Rights. These rights are detailed below. This list table of user rights is quoted from the SANS Institute Windows NT 4.0 Security: Step-by-Step book:

User Right	Possible Problems	Domain Controller	Standalone/ Member Server	Professional
Access this computer from the network	Stolen administrator accounts can be used over the network. Removing the right from the administrator accounts forces these users to have physical access to the system in order to access resources.	Domain Users (remove Administrators from this right)	Domain Users	None
Act as part of the operating system	Acting as part of the operating system overrides all other rights, permissions, or privileges.	None	None	None
Add workstations to the domain	Users with this right could add another domain controller to the network and obtain a copy of the SAM database.	Administrators Custom*	None	None
Backup files and directories	Users with no permissions for certain files or folders can make backup copies. When combined with the Restore Files and Directories right, this right can allow unauthorized users to obtain copies of critical files.	Backup Operators	Backup Operators	Backup Operators
Bypass traverse checking	Allows access to files or folders regardless of the user's permissions to the parent folder. In other words, prevents the inheritance of permissions.	Administrators, Server Operators, and Backup Operators	Administrators ("Users" seems to be required for IIS)	Administrators
Change the system time	Resetting the system time can seriously impact or destroy audit trails. System time can effectively disable Kerberos security.	Administrators	Administrators	Administrators and Power Users
Create a pagefile		Domain Admins	Administrators	Administrators

Create a token object	Allows the creation of a security access token. This right should never be given to any user.	None	None	None
Create permanent shared objects				
Debug programs	Allows the user to debug other processes and threads. Users with this right could modify programs to run malicious code.	None (except in off-Internet development)	None (except in off-Internet development)	None (except in off-Internet development)
Force shutdown from a remote system				
Generate security audits				
Increase quotas				
Increase scheduling priority	This allows a user to increase the priority of a process. Setting a process's priority too high, can consume system resources creating a denial of service attack.	Administrators	Administrators	Administrators
Load and unload device drivers	Granting this right to a user could allow a Trojan Horse device driver to be loaded.	Administrators	Administrators	Administrators
Lock pages in memory	A user could use this right to launch a denial of service attack.	None	None	None
Log on as a batch job				
Log on as a service	The user could log on as a service with full control of the system. Some accounts, such as virus scanners, require this right and should be closely monitored.	Replicators	None	None
Log on locally	Known security bugs (such as GetAdmin) can escalate users permissions if run from the local console.	Administrators Server Operators and Backup Operators	Administrators Server Operators and Backup Operators	Administrators and Authenticated Users

Manage auditing and security log	Allows viewing and clearing of the audit logs. An attacker could clear the security log to erase evidence of the attack.	Administrators	Administrators	Administrators
Modify firmware environment values	Environment variables can be modified to point to malicious programs.	Administrators, Server Operators, and Backup Operators	Administrators	Administrators
Profile single process				
Profile system performance				
Replace a process level token	A user with this right could replace a security access token of a process with a different token.	None	None	None
Restore files and directories	Users with this right can restore files regardless of their permissions. If a user has both the Backup and Restore rights, the user could backup a malicious file from one location and use it to overwrite critical system files or to plant a backdoor. In high security environments, the Backup and Restore rights should not be given to the same users. In many systems, however, this is not a viable solution.	Backup Operators, or create a custom "Restore Operators" group.	Backup Operators, or create a custom "Restore Operators" group.	Backup Operators, or create a custom "Restore Operators" group.
Shut down the system	Users could bring the system down in the middle of critical jobs or while users are accessing system resources.	Administrators and Server Operators	Administrators	Authenticated Users
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

* A custom group for Desktop Support Personnel should be created. This right can potentially be dangerous, but needs to be expanded beyond just administrators to be functional in a domain.

Appendix C: Change History

January 25, 2002 – Draft Version v0.9.0 released.
March 1, 2002 – Draft Version 0.9.2 released.
April 1, 2002 – First Public Release: Version 1.0.2 released.
April 16, 2002 – Version 1.0.3 released.
Fixed misplaced settings in Account Lockout Policy table.
August 28, 2003 – Released new Terms of Use.