UCRL MA130381

Windows NT 4.0 Workstation Security Advisor

version 1.3

compiled by
James Rothfuss
May 27, 1998

Work performed under the auspices of the U. S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

Acknowledgments

I would like to thank the following folks for their review and subsequent suggestions and corrections concerning this document: Philip Cox, James Guse, Howard Guyer, Teena Henson, John A. Hernandez, Jerry Rayome, Norman Samuelson

–

Lawrence Livermore National Laboratory

Table of Contents

I. Document Scope

The target audience is the casual user of Windows NT Workstation who has connected their computer to a possibly hostile network, like the Internet, and has little intention of offering major network services from their workstation.

I have had to draw a fuzzy line between security and system administration. This is a security document, so, while I have tried to address security issues with specific detail, I have ignored many system administration functions that have security implications (i.e. how to add and manage accounts, how to use the registry editor, or how to do backups). Some knowledge of managing a Windows NT system is assumed.

This document is written for the Workstation version of Windows NT. Security issues specific to Windows NT Server are not addressed. Much of the guidance can apply to the Server version, but there are more issues that need to be considered when trying to secure a Server.

Many suggestions are made with the assumption that the workstation will offer few, if any, network services. Examples of network services that can be run on Windows NT Workstation are file sharing (shares), the Personal Webserver, FTP, Telnetd. If all of the security recommendations in this document are strictly followed, many network services will not work.

Windows NT is a versatile operating system with many options. **Each user needs to use some judgment in assessing if the suggestions made by this document will work within their own environment.**

II. Recommendation Key

I have associated a security, operational, and implementation impact with each suggestion. My intent is to give a concise indication of importance versus cost. However, these are subjective assessments and may not apply in all situations.

Security Impact:	Necessary	- Required for a secure system[1]
	Recommended	- Not required, but probably should be implemented.
	Optional	- Should be considered as a extra safeguard.
	Evaluate	- May add security in some environments, but may be detrimental in others.
Operation Impact:	High	- The operational impact may be significant enough to outweigh the security benefit.
	Medium	- Some type of operational impact will result.
	Low	- Little or no impact will result.
	Evaluate	- Operational Impact will vary from low to high, depending on the environment and may require a risk/impact decision.
Implementation:	Involved	- May take significant time and/or ability to implement.
	Simple	- Not difficult, but may take some time.
	Very Easy	- Easily implemented.

If a known negative result might be created by the implementation of a suggestion, a warning about that result is emphasized with the warning symbol:


Warning

[1] The statement "Required for a secure system" should not be interpreted as "Required for a functional system". Many fully functional systems are run with the risk acceptance of open vulnerabilties.

III. References

The next three references were used extensively in creating this document:

Sheldon, Tom *Windows NT Security Handbook* Osborne McGraw-Hill, 1997. ISBN 0--7-882240-8

Microsoft Windows NT Workstation Resource Kit Microsoft Press, 1996. ISBN 1-57231-343-9

Securing Windows NT Installation White Paper Microsoft Corporation, October 23, 1997
http://www.microsoft.com/ntserver/guide/secure_ntinstall.asp
(Note: Must use MSIE to view this site, Netscape does not work)

Microsoft Knowledge Base articles (referenced by QXXXXXX numbers) are available at:
ftp://ftp.microsoft.com/bussys/winnt/kb
or go to http://www.microsoft.com and use their search facility to find the article.

The following is a list of more Websites for further information about Windows NT security:

http://www.microsoft.com/security/
http://www.ntsecurity.net/
http://www.versalink.com/ntmain.htm
http://www.iss.net/vd/sitesn.html
http://www.iss.net/vd/nt_vulnerabilities.html
http://www.somarsoft.com/security.htm

IV. Service Packs and Hot Fixes

A. Install the latest Service Pack

Security Impact:	Necessary
Operation Impact:	Low
Implementation:	Involved

Service Packs (SP) correct problems with the Windows NT operating system and often fix security relevant "bugs". Each SP incorporates the bug fixes from the previous ones, so only the latest SP needs to be installed.

Install the latest recommended Microsoft SP for the NT operating system. As of March 1998, SP3 is the latest.

FTP to one of the following sites:
ftp.microsoft.com/bussys/winnt/winnt-public /fixes/usa/nt40/ussp3/
or
198.105.232.37/fixes/usa/nt40/ussp3/
Download and read the README file.
Download and install SP3 as per the instructions.

To determine the latest SP that has been installed on a system, use the WINVER command

From the Start Pulldown, select RUN.
Enter WINVER.
Click OK.

Warning Windows NT version 4.0 Service Pack 3 includes enhancement to Server Message Block (SMB) file sharing protocol such that by default you are unable to connect to SMB servers (such as Samba or Hewlett-Packard (HP) LM/X or LAN Manager for UNIX) with an unencrypted (plain text) password. This protects from sending clear text forms of passwords over the wire. Please refer to Knowledge base article Q166730 if you have any reasons to allow clients to send unencrypted passwords over the wire.

B. Install applicable Hot Fixes

Security Impact:	Necessary
Operation Impact:	Low
Implementation:	Involved

The applicable hot-fixes should also be installed. Generally not all hot-fixes are required. Also the order in which hot-fixes are installed is very important, as later hot-fixes sometimes supersede earlier hot-fixes.

The table in Appendix A "Hot Fixes for Service Pack 3 as of April 1998" on page 41 gives brief descriptions of Hot Fixes. If you are not using the service, program, or hardware that the Hot Fix addresses, there is no need to install the Hot Fix. Be sure to read the README files and MS Technical Documents before installing the Hot Fix. More information about security relevant Hot Fixes can be obtained at http://www.microsoft.com/security.

FTP to one of the following sites:
ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/
or
198.105.232.37/fixes/usa/nt40/hotfixes-postSP3/ (Note: This site is not as current as ftp.microsoft.com, but is reported to be faster)
Read postsp3.txt for the sequence that should be used when installing multiple Hot Fixes
Go to the directory for the desired Hot Fix.
Download and read the README file.
Download and install the Hot Fix as per the instructions.

There are two ways to determine what Hot Fixes have already been installed.

The first way is to use the hotfix.exe utility that comes bundled with the Hot Fixes. To obtain hotfix.exe do the following:

Download a recently released Hot Fix (older Hot Fixes have an older version of hotfix.exe that does not have the "list" fuctionallity).
Extract the files from the Hot Fix using the /x qualifier:

```
C:\> hot-fix-name /x
```

One of the files extracted will be hotfix.exe.
Run hotfix.exe with the -l (list) qualifier:

```
C:\> hotfix -l
```

A list of the Qxxxxxx knowledge base articles associated with the Hot Fixes will be listed.

The second way is to examine the registry keys:

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	Microsoft\Windows NT\CurrentVersion\Hotfix\Qxxxxxx
Name:	Comments or Fix Description

V. User Manager

A. Change the name of the Administrator and Guest accounts

Security Impact:	Necessary
Operation Impact:	Low
Implementation:	Very Easy

Rename the built-in Administrator and Guest accounts to something less obvious. The Administrator account is a powerful account that normally cannot be locked out, and consequently is attractive to hackers who try to break in by repeatedly guessing passwords. The Guest account is not as powerful and can be locked, but renaming it adds an extra level of protection. By renaming these accounts, you force hackers to either guess the account name or use more sophisticated methods to obtain it.

Run User Manager.
Single click the Administrator account.
Pulldown the User menu and select Rename.

Warning Some third party utility programs that need to be run under a privileged account will not run unless that account is called Administrator.

B. Disable the Guest account

Security Impact:	Necessary
Operation Impact:	Low
Implementation:	Very Easy

In most cases, individual accounts for each user should be created. If this is done the Guest account becomes an unnecessary vulnerability. By default, the built-in Guest account does not have a corresponding password and will allow anyone to logon as Guest. The Guest account cannot be removed, but it can be disabled. Giving the account a difficult password in addition to disabling it gives another layer of protection.

Run User Manager.
Double click the Guest account.
Check the Account Disabled check box.
Give the account an extremely difficult 14 character password.

C. Create a “decoy” account for Administrator

Security Impact:	Recommended
Operation Impact:	Low
Implementation:	Simple

Create a disabled “decoy” account called “Administrator” which has no rights. This decoy account will act as an alert for many types of break-in or scan attempts if unsuccessful login attempts are being monitored (see “Set auditing for Logon and Logoff success and failure” on page 15).

Do the following after renaming the real Administrator account:

Run User Manager.
Pulldown the User menu and select New User.
Type in Administrator in the Username window.
Check the Account Disabled check box.
Give the account an extremely difficult 14 character password.

Another approach is to severely restrict access within the decoy account's environment by using the Profile Editor (POLEDIT.EXE) from the Workstation Resource Kit. Allowing the attacker to actually break the account may result in more information about the attacker's techniques. However, considerable care must be taken to insure that the account has been completely isolated. The severely restricted account method is not recommended unless you have a thorough knowledge of NT security. In addition, it should only be done on relatively unimportant hosts. Never allow an attacker to remain connected to an important production machine.

D. Check default user rights

Security Impact:	Necessary
Operation Impact:	Low
Implementation:	Involved

The rights listed in Appendix B "Suggested workstation user rights" on page 44 are the general default settings. Walk through the list and check that the defaults are correct. It is recommended that rights be restricted as severely as is possible for a particular environment.

Run User Manager.
Pulldown the Policies menu and select User Rights.
Check mark Show Advanced User Rights.
Step through each Right, examining who it is granted to.

E. Disable network logon privileges for the Administration account

Security Impact:	Optional
Operation Impact:	Medium
Implementation:	Simple

Removing the right **Access this computer from the network** from the Administration Account and all groups that the Administration account belongs to will block Administrator account access from the network and will greatly reduce network vulnerability.

Run User Manager.
Pulldown the Policies menu and select User Rights.
Choose the right: Access this computer from the network.
Single click on the administration account in the "Grant to:" window.
Single click the Remove button.
Similarly, remove all groups that the Administrator account belongs to (including the Everyone Group).

Warning

1) Disallowing administration access over the network will remove the ability to do most administrative function over the network.

2) The telnetd service provided with the Resource Kit does not block access based on the **Access this computer from the network** right. There may be other layered network services that are not blocked.

F. Disable network logon privileges for the Everyone group

Security Impact:	Necessary
Operation Impact:	Low
Implementation:	Very Easy

Removing the right **Access this computer from the network** from the Everyone Group will limit network access to those accounts and groups that have expressly been given network rights. Removing this access from Everyone will reduce network vulnerability.

Run User Manager.
Pulldown the Policies menu and select User Rights.
Choose the right: Access this computer from the network.
Single click on Everyone in the "Grant to:" window.
Single click the Remove button.

Warning

The telnetd service provided with the Resource Kit does not block access based on the **Access this computer from the network** right. There may be other layered network services that are not blocked.

G. Restrict local (console) logons

Security Impact:	Recommended
Operation Impact:	Low
Implementation:	Simple

The right **Log on locally** allows a user to log on at the computer, from the computer's console. Remove this right from Everyone, Guests, and any other users or groups that do not need access to the workstation from the console. This is a precaution that further restricts users that have no specific rights.

Run User Manager.
Pulldown the Policies menu and select User Rights.
Select the Restrict Local Logons right.
Select and remove Everyone from the Grant To window.
Select and remove Guests from the Grant To window.

H. Restrict system shutdown

Security Impact:	Optional
Operation Impact:	Evaluate
Implementation:	Simple

The right **Shut down the system** (SeShutdownPrivilege) allows a user to shut down Windows NT. If your environment dictates that only designated system administrators should have strict control over the management of the computer, remove Everyone, Guests, and other users from having this right.

Run User Manager.
Pulldown the Policies menu and select User Rights.
Choose the right: Shut down the system.
Select and remove Everyone from the Grant To window.
Select and remove Guests from the Grant To window.
Select and remove Users from the Grant To window.

I. Set password policy

Security Impact:	Necessary
Operation Impact:	Low
Implementation:	Very Easy

The following settings will insure that users:

1) occasionally change their passwords

2) do not use short passwords

3) do not reuse old passwords

4) do not change their password several times in a short period of time, thus allowing them to reuse their old password.

The numbers shown (180, 8, 24, 1) in the following example are recommended.

Run User Manager.
Pulldown the Policies menu and select Account.
Set Maximum Password Age to expire in 180 days.
Set Minimum Password Length to at least 8 characters.
Set Password Uniqueness to remember 24 passwords.
Set Minimum Password Age to allow changes in 1 day.

For stronger enforcement of passwords, see “Enforce strong user passwords” on page 31

J. Set account lockout policy

Security Impact:	Necessary
Operation Impact:	Low
Implementation:	Very Easy

Locking out failed login attempts will prevent automated, brute force, password attacks against accounts. The numbers shown (5,5,10) in this example are recommended.

Run User Manager.
Pulldown the Policies menu and select Account.
Check the Account Lockout radio button.
Set lockout after 5 bad logon attempts.
Set reset count after 5 minutes.
Set lockout duration 10 minutes.

Warning

The lockout policy only works reliably for logins from other Windows NT clients. If other login avenues have been setup (such as a third party telnet service), they may not recognize the lockout policy.

K. Force users to log on in order to change password

Security Impact:	Optional
Operation Impact:	Medium
Implementation:	Very Easy

Normally, if the password expires, users can login and will be presented with a password change dialog box. If “User Must Log On” option is selected, the user will not be able to change their own password and will need the assistance of a system administrator.

Run User Manager.
Pulldown the Policies menu and select Account.
Check the Account Lockout radio button.
Check the User Must Log On In Order To Change Password check box.

L. Give rights to local groups, not to users

Security Impact:	Recommended
Operation Impact:	Low
Implementation:	Simple

Giving rights to a specific user or to a group to which the user belongs both have the same effect on the user’s capabilities. However, as the number of users increase, managing rights for each individual user becomes increasingly difficult. It is almost always more advantageous to assign users to a group or groups that have been granted the desired rights. The assumption is that the number of groups will always be significantly less than the number of users and therefore, easier to manage.

To create a new Group:

```
Run User Manager.
Pulldown the User menu and select Add Local Group.
Fill out the Local Group pop up window as desired.
```

To add users to an existing group:

```
Run User Manager.
Double click the user name.
Click the Groups button.
Add the desired groups.
```

To add rights to Groups

```
Run User Manager.
Pulldown the Policies menu and select User Rights.
Select the desired right.
Add the group to the Grant To window.
```

M. Set permissions on objects for groups, not users

Security Impact:	Recommended
Operation Impact:	Low
Implementation:	Simple

Giving object permissions to a specific user or to a group to which the user belongs both have the same effect on the user's access to the object. However, as the number of users increase managing object permissions for each individual user becomes increasingly difficult. It is almost always more advantageous to assign users to a group or groups that have been granted the desired permissions. There are two assumptions. The first is that the number of groups will always be significantly less than the number of users and therefore, easier to manage. The second is that users will come and go, but groups will stay relatively constant. Permissions on individual objects will not have to be changed as the user population changes.

To create a new Group:

```
Run User Manager.
Pulldown the User menu and select Add Local Group.
Fill out the Local Group pop up window as desired.
```

To add users to an existing group:

```
Run User Manager.
Double click the user name.
Click the Groups button.
Add the desired groups.
```

To add permissions to an object:

Right click on the object and select Properties.
Select the Security tab on the Properties popup window.
Click the Permissions button.
Add desired groups with desired permissions.

N. Set auditing for Logon and Logoff success and failure

Security Impact:	Necessary
Operation Impact:	Low
Implementation:	Very Easy

Audit logs are valuable tools for detecting and recovering from security incidents. The recommended events for auditing are:

1) Logon and Logoff success and failures

2) Successful and Unsuccessful changes to user and group accounts

3) Successful and Unsuccessful changes to security policy

Note: For the detection aspect of audit logs to be effective, they must be examined on a regular basis.

Another Note: Auditing only works reliably for logins from other Windows NT clients. If other login avenues have been setup (such as a third party telnet service), they may not audit properly.

Run User Manager.
Pulldown the Policies menu and select Audit.
Pick Audit These Events.
Check Success and Failure for Logon and Logoff.
Check Success and Failure for User and Group Management.
Check Success and Failure for Security Policy Changes.

To view the logs

Run Event Viewer.
Pulldown the Log menu and select Security.
Double click on any event entry for more information about the event.

The Windows NT Resource Kit contains an on-line Help package AUDITCAT.HLP. This help package describes all of the audit categories, including the event numbers associated with each event.

Note: If “File and Object Access” Events are to be monitored, each file or object to be monitored must have auditing enabled in the security properties.

Right click on the file or object.
Pick the Security tab (this will only show up for NTFS file systems).
Click the Auditing button.
Use the Add button to add users and groups whose access will be monitored.
Check the types of access to be monitored.

Warning Auditing uses disk space which, depending on the amount of disk space available, must be cleared occasionally.

Run Event Viewer.
Pulldown the Log menu and select the log to clear (System, Security, Application).
Pulldown the Log menu and select Clear All Events.

VI. Control Panels

A. Use the locking screensaver

Security Impact:	Recommended
Operation Impact:	Medium
Implementation:	Very Easy

Users should either log off or lock the workstation if they will be away from the computer for any length of time. The workstation can be set to lock automatically if it is not used for a set period of time by using any 32-bit screen saver with the Password Protected option.

Right click on a "blank" area of the screen and select Properties or select Display from the Control Panel.
Select the ScreenSaver tab on the Properties popup window.
Select the desired screen saver.
Enter the desired wait time.
Check the Password Protected box.

The screensaver will use the users normal logon password.

B. Disable the startup of services that are not being used

Security Impact:	Evaluate
Operation Impact:	Evaluate
Implementation:	Involved

Windows NT runs Services as background processes that add functionality to the Windows NT operating system. Most Services involve network interactions. Many Services may be started by default, even if the functionalities they provide are never used. If it can be determined that a Service is never used, turning off that Service may reduce the opportunity for system intrusion. (Example: if you never view your clipboard from another workstation, you don't need Clipboard Viewer turned on)

Select Service from the Control Panel.
Click on the service to adjust.
Click the Startup button (or double click on the service).
Select the type of startup:
Automatic - will start at boot
Manual - must be started through the control panel
Disabled - Cannot be started

C. Remove Alerter and Messenger services

Security Impact:	Optional
Operation Impact:	Evaluate
Implementation:	Very Easy

The Windows NT Alerter and Messenger services enable a user to send pop-up messages to other users. A network administrator may consider this an unnecessary risk due to the fact that these types of services have been known to be used in social engineering attacks. Some users might actually respond to a

request to change their password, create a share, or otherwise open holes in the network. A side effect of running this service is that it causes the name of the current user to be broadcast in the NetBIOS name table, which gives the attacker a valid user name to use in brute force attempts.

Select Service from the Control Panel.
Click on the Alerter service.
Click the Startup button (or double click on Alerter).
Select the Disable button.
Disable the Messenger service in the same manner.

D. Only bind network protocols as necessary

Security Impact:	Optional
Operation Impact:	Evaluate
Implementation:	Simple

Some network services are bound to network protocols, which are in turn bound to hardware adapters. The common services that usually bind to the network protocols are the NetBIOS interface, Server, and Workstation. By default these are bound to the NetBEUI protocol. When other protocols (such as TCP/IP) are added, the services will usually automatically bind to the added protocol.

If a protocol is not being used by a service, the binding may present an unnecessary vulnerability and should be disabled.

Example: If the workstation is connected to the internet, TCP/IP must be installed to allow internet connections (web browsers, telnet, ftp). However if the Server service, which is used to share Windows file systems, is bound to TCP/IP, filesystems might be shared across the whole internet. An easy way to share filesystems locally, but insure that they will not be shared across the internet, is to unbind Server from TCP/IP and bind it to a non-routeable protocol such as NetBEUI.

From the Control Panel, select Network.
Select the Bindings tab on the Network popup window.
Double click on the interface (NetBIOS, Server, or Workstation).
Select the binding to disable.
Click the Disable button.

VII. Performance Monitor

A. Set alarms for excessive network activity

Security Impact:	Evaluate
Operation Impact:	Medium
Implementation:	Involved

Excessive incoming network activity may indicate a denial of service attack. The first step is to determine a baseline for the normal amount of traffic by monitoring the system for a few days. To accomplish this, perform the following:

Run Performance Monitor.
Pulldown View and select Log.
Pulldown Edit and select Add To Log.
Select Network Interface as the Object to monitor.
Pulldown Options, select Data From, Click on Current Activity.
Pulldown Options and select Log.
Enter a logfile name.
Enter an appropriate interval (shorter intervals will log more accurate information, but will fill the logfile faster.
Click the Start button.

After the data is collected, determine the peak network activities.

Run Performance Monitor.
Pulldown View and select Chart.
Pulldown Options and select Data From.
Click on Log File and enter the logfile name.
Pulldown Edit and select Add To Log.
Select Network Interface as the Object.
Select Bytes Received/Sec as the Counter to monitor.

A chart of the logged data will appear. This chart is compressed and averaged, so the maximum reported may not reflect the real maximum. Use the Alert function to find the real maximum recorded.

Note the Maximum value reported on the chart.
Pulldown View and select Alerts.
Pulldown Options and select Alerts.
Set the Interval at least as low as the interval at which the logfile was recorded.
Pulldown Edit and select Add To Alert.
Select Network Interface as the Object.
Select Bytes Received/Sec as the Counter to monitor.
Click on Alert If Over and enter the maximum value noted earlier.
Click Add.
Determine the maximum value by reviewing the Alerts.

Once the maximum Network Bytes Received/second has been determined use that number to estimate a higher value which will be used as an alarm. Set the alarm at that value.

Pulldown Options and select Data From.
Click on Current Activity.
Pulldown Edit and select Add Alert.
Reconstruct the Alert with the new alarm value.
Pulldown Options and select Alert.
Set the options with the desired type of notification (to send a popup notification to the screen, enter the name of the workstation as the Net Name).
Pulldown File and Save Alert Settings into a .PMA file.

Use the Monitor program from the Resource Kit to activate continuous monitoring of the alarm.

Copy the file DATALOG.EXE from the Resource Kit into the %SYSTEMROOT%\SYSTEM32\ directory.
From the DOS prompt:

```
C:\> monitor startup
C:\> monitor filename.PMA
C:\> monitor automatic
C:\> monitor start
```

B. Set alarms for various server errors

Security Impact:	Optional
Operation Impact:	Medium
Implementation:	Involved

The following items can be monitored for alarm situations. These only apply to network connections connecting through the Windows NT server function.

- Errors Access Permissions
- Errors Granted Access
- Errors Logon

Run Performance Monitor.
Pulldown View and select Alert.
Pulldown Edit and select Add To Alert.
Select Server as the Object to monitor.
Select Errors Access Permissions for the Counter.
Click on Alert If Over and enter an appropriate value.
Click Add.
Set the options with the desired type of notification (to send a popup notification to the screen, enter the name of the workstation as the Net Name).

Create alerts for Errors Granted Access and Errors Logon using the same steps outlined above. Save the alert settings in a file:

Pulldown File and Save Alert Settings into a .PMA file.

Use the Monitor program from the Resource Kit to activate continuous monitoring of the alarm:

Copy the file DATALOG.EXE from the Resource Kit into the %SYSTEMROOT%\SYSTEM32\ directory.
From the DOS prompt:

```
C:\> monitor startup
C:\> monitor filename.PMA
C:\> monitor automatic
C:\> monitor start
```

Some TCP network connections, such as the telnetd service supplied in the resource kit are not detected. For these connections, set up alarms using the TCP Object and the Connection Failures counter.

VIII. File System Security

A. Format disk with NTFS

Security Impact:	Necessary
Operation Impact:	Low
Implementation:	Involved

The NTFS file system provides more security features than the FAT system and should be used whenever security is a concern. The only reason to use FAT is for the boot partition for Windows 95 or an ARC-compliant RISC system.

With NTFS, you can assign a variety of protections to files and directories, specifying which groups or individual accounts can access these resources in which ways. By using the inherited permissions feature and by assigning permissions to groups rather than to individual accounts, you can simplify the chore of maintaining appropriate protections.

To convert a FAT file system on Disk C: to NTFS, use the following command:

```
C:\> convert C: /FS:NTFS /v
```

If the disk is in use and the conversion cannot be done immediately, you will be given the option to have the disk converted when Windows NT reboots.

The File System option of the C2CONFIG utility can also be used to convert file systems. See “C2CONFIG utility” on page 37

Warning **1)** There is no easy way, short of reformatting the disk to convert back to the FAT file system.

2) DOS, Windows 3.x, and Windows 95 do not recognize the NTFS file system, so NTFS files become inaccessible if the system is booted from a DOS boot floppy.

B. Secure FAT file systems on RISC based systems

Security Impact:	Recommended
Operation Impact:	Evaluate
Implementation:	Involved

On RISC based systems the FAT file system must be used. To secure the system partition do the following:

```
Use the Disk Administrator Utility.
Pulldown the Partition menu and select Secure System Partition.
```

C. Set NTFS file permissions to recommended values

Security Impact:	Necessary
Operation Impact:	Low
Implementation:	Involved

If a FAT file system is converted to NTFS, the permissions on all files will be FULL ACCESS to Everyone. Even if the file system has already been converted to NTFS by the manufacturer, the file permissions are often left in a vulnerable state (especially on Workstations).

Set directory permissions to all subdirectories and existing files, as shown in Appendix D "Recommended folder and file permissions" on page 46, *immediately after Windows NT is installed*. Permissions must be applied to parent directories before applying permissions to subdirectories.

To apply permissions:

Select the directory with the right mouse button.
Select properties.
Select the Securities tab.
Click the Permissions button.
Add, Modify, or Delete permissions as needed.
Check mark Replace Permissions on Sub-directories.
Check mark Replace Permissions on Existing Files.
Click the OK button.

The File System Security option of the C2CONFIG utility can also be used to set strong permissions on NTFS files. See "C2CONFIG utility" on page 37. The file C2NTFACL.INF controls the permissions set by C2CONFIG.

Warning If layered software has been added to the NT operating system and these recommended permission changes are made, some of the changes may extend into the layered software's files, causing problems with the software's operation.

D. Separate executable and data into separate folders

Security Impact:	Recommended
Operation Impact:	Evaluate
Implementation:	Involved

Whenever possible, place executable program files in different directories than data files. Only give user accounts READ/EXECUTE(RX) permission to the program directory and files. This will prevent users from intentionally or accidentally introducing virus and/or trojan horse programs into program files.

E. Use Change permissions on folders instead of Write

Security Impact:	Recommended
Operation Impact:	Evaluate
Implementation:	Involved

In cases where programs require files (such as temp files) to be written into the executable's directory, give the directory CHANGE permission, but leave all initial files in the directory READ/EXECUTE only.

F. Give administrators Change permission instead of Write

Security Impact:	Recommended
Operation Impact:	High
Implementation:	Involved

If administrators automatically have write permission to most files on the system, they can inadvertently infect vast numbers of files with viruses or trojan horses. By changing the permission to CHANGE (especially on executable files), the administrator will have to take the extra step of adjusting permissions in the cases

where they must change the existing files. A malicious program trying to modify other files will probably not take this extra step and the failed attempt to modify will alert the administrator.

G. Use Change permission instead of Full Control

Security Impact:	Recommended
Operation Impact:	Evaluate
Implementation:	Involved

If RX is not enough permission for successful execution, try using CHANGE permission before resorting to FULL CONTROL.

H. Use strong permissions on shares

Security Impact:	Necessary
Operation Impact:	Low
Implementation:	Simple

When a file share is created, by default the permission is Everyone:FULL CONTROL. This permission is rarely a prudent choice. Select permissions that will restrict access to the share as much as possible without negating the purpose of the share.

Right click on folder to be shared.
Select Properties from the pulldown menu.
Select the Sharing tab.
Click on Share As.
Click the Permissions button.
Remove or modify the Everyone access.
Add other access as required by the share's intended use.

IX. Registry Modifications

Warning Changing some registry keys inaccurately can result in disastrous results. The system may not boot, or, if it does boot, some functionality may be lost. Be sure to create an Emergency Recovery Disk (ERD) using the RDISK utility (run from the DOS prompt) before making registry changes.

```
C:\> RDISK /S
```
The /S switch instructs the ERD to save the entire registry.

It is also advisable to make backups of the registry using the REGBACK utility from the Workstation Resource Kit.

Note: The Windows NT BACKUP utility does not backup the registry unless the “Backup Local Registry” option is selected. This option is not selected by default.

After registry changes are made and the system is stable, make a new ERD.

The C2CONFIG and POLEDIT utilities in the Workstation Resource Kit can be used to implement many of these features without using the registry editor.

A. Protect registry keys

Security Impact:	Necessary
Operation Impact:	Evaluate
Implementation:	Involved

By default Windows NT installs with reasonable protections on registry keys. The registry keys should be spot checked to see if protections have not been changed to something unreasonable (i.e. EVERYBODY:FULL CONTROL). The SECURITY and SAM keys should be unavailable to all users, even the Administrator account.

Run REGEDT32.
Select a key.
Pulldown the Security menu and select Permissions.
Adjust permissions in the popup window.

For better security on registry keys, consider the recommendations in Appendix E “Highly secure registry protections” on page 48.

In the recommendations that follow, after setting the key values, check that the security on this key is set to disallow everyone other than Administrators and System any access. Otherwise malicious users can reset these values.

The Registry Security option of the C2CONFIG utility can also be used to protect registry keys. See “C2CONFIG utility” on page 37. The file C2REGACL.INF controls the permissions set on registry keys by C2CONFIG.

Warning Some caution should be exercised when changing registry key permissions since programs often need to access certain keys on the user’s behalf. If you have recently changed registry protections, and an application starts to “break”, check protections on registry keys that the application uses.

B. Disable LanManager password hash support

Security Impact:	Optional
Operation Impact:	Evaluate
Implementation:	Simple

Two types of challenge/response authentication are supported by Windows NT; LanManager (LM) challenge/response and Windows NT challenge/response

The LM authentication is used to allow service connects to Windows 95, Windows for Workgroups, and SAMBA platforms. To allow access to these servers, Windows NT clients, by default, send both authentication types. If your environment is entirely Windows NT, LM is not needed and presents an additional avenue of attack.

Apply Service Pack 3 and then the lm-fix Hot Fix (see Appendix A, page 41) to configure the following registry key:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Control\LSA
Name:	LMCompatibilityLevel
Type:	REG_DWORD
Value:	0,1, or 2

- The value of 0 will send both Windows NT and LM password forms (default).
- The value of 1 will send Windows NT and LM password forms only if the server requests it.
- The value of 2 will never send the LM password form.

C. Restricting anonymous access

Security Impact:	Optional
Operation Impact:	Evaluate
Implementation:	Simple

The anonymous login account is a “hidden” account that is used for some network operations. Windows NT has a feature where this account can list domain user names and enumerate share names over the network. Allowing the anonymous account to list this information may allow intruders to gain infiltration knowledge about your Workstation. Windows NT 4.0 Service Pack 3 provides a mechanism for administrators to restrict this ability.

Set the following value to disallow anonymous access:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Control\LSA
Name:	RestrictAnonymous
Type:	REG_DWORD
Value:	1

Knowledge Base article Q143474 has more details about restricting anonymous access.

Warning Listing account names from Domain Controllers is required by some network utilities. For example, the Windows NT ACL editor obtains lists to grant access rights and the Windows NT Explorer selects from lists to grant access to shares. If these facility and other similar facilities are used over the network, anonymous account lookup may be necessary.

A list of named pipes can be excluded from network restrictions by using the following registry key:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Services\LanManServer\Parameters
Name:	NullSessionPipes
Type:	REG_MULTI_SZ
Value:	Add or Remove names from the list as required by the configuration.

Unless a network application demands an anonymous session, remove all values from this string. For more information refer to Knowledge Base article Q143138.

D. Audit base objects

Security Impact:	Evaluate
Operation Impact:	Evaluate
Implementation:	Simple

In addition to Files, Registry Keys, and Printers, Windows NT has a number of objects that are generally not visible to or known by a typical user. Application programmers learn about these objects in software development kits and use them to exploit the system.

Auditing these objects can introduce many unwanted audit entries. However, in some situations, it might be desirable to audit accesses to base objects. For example, when custom applications are being developed, the “users” are programmers. These programmers might be able to directly access the base objects.

To enable auditing on base system objects, add the following key value to the registry key

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Control\Lsa
Name:	AuditBaseObjects
Type:	REG_DWORD
Value:	1

In addition to setting this key the administrator will need to set auditing on for the “Object Access” category using User Manager. By setting this registry key, the Local Security Authority will create base objects with a default system audit control list.

E. Audit use of privileges

Security Impact:	Evaluate
Operation Impact:	High
Implementation:	Simple

To control the growth of audit logs, some privileges are not audited, even when auditing Privilege Use is turned on. The privileges are:

Bypass traverse checking (given to Everyone).	Since this is granted to Everyone, auditing it is not of any value.
Debug programs (given only to administrators)	Usually not used in production system.
Create a token object (given to no one)	Highly sensitive privilege that is usually not granted to any user or group.
Replace process level token (given to no one)	Highly sensitive privilege that is usually not granted to any user or group.
Generate Security Audits (given to no one)	Highly sensitive privilege that is usually not granted to any user or group.
Backup files and directories (given to Administrators and Backup Operators)	Used often during normal system operations.
Restore files and directories (given to Administrators and Backup Operators)	Used often during normal system operations.

To enable auditing of these privileges, add the following key value to the registry key:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Control\Lsa
Name:	FullPrivilegeAuditing
Type:	REG_BINARY
Value:	1

Warning Backup and restore operations is a frequent check privilege use for every file and directory backed or restored leading to thousands of audits filling up the audit log.

F. Cause shutdown when audit log is full

Security Impact:	Evaluate
Operation Impact:	High
Implementation:	Simple

An option is provided that will cause the system to shut down if the security audit log fills up. To enable this, use the following key value in the registry key:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Control\Lsa
Name:	CrashOnAuditFail
Type:	REG_DWORD
Value:	1

If the a full audit log causes the system to shutdown, this value in the registry is reset to 2. When the value is set to 2, only users in the administrators group will be allowed to log onto the machine (locally or remotely). They can then empty the audit log by deleting it or archiving it and reset the value to 1. A reboot is necessary before any other users are allowed to log on.

The Halt on Audit Failure option of the C2CONFIG utility can also be used to cause the shutdown. See "C2CONFIG utility" on page 37

Warning If audit logs are crucial to your environment, this option may be necessary. However, it can also be used for a denial of service attack by forcing network activities that will fill up the audit log and cause an unexpected shutdown.

G. Secure Server Message Block (SMB) protocol

Security Impact:	Recommended
Operation Impact:	Evaluate
Implementation:	Simple

SMB is the primary protocol Windows NT uses to share files over the network. Starting with Service Pack 3 message signing, verified by both server and client ends, is incorporated into SMB packets. This mutual authentication counters man-in-the-middle attacks and active message attacks. These features are not set by default.

To cause Servers to require secure signatures for connections, configure the following key value:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Services\LanManServer\Parameters
Name:	RequireSecuritySignature
Type:	REG_DWORD
Value:	1

Similarly, to cause clients to only connect to servers that support message signing, configure the following key value.

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Services\Rdr\Parameters
Name:	RequireSecuritySignature
Type:	REG_DWORD
Value:	1


Warning

If these values are set, the server or client will only communicate with those servers or clients that are aware of message signing. This means that older versions of Windows NT (pre-service pack 3) will not connect.

The Knowledge Base article Q161372 has more details.

H. Secure print driver installation

Security Impact:	Recommended
Operation Impact:	Evaluate
Implementation:	Simple

Registry key AddPrinterDrivers is used to control who can add printer drivers using the print folder. Setting the key value to 1 will restrict this operation to administrators and power users.

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentcontrolSet\Control\Print\Providers\LanMan Print Services\Servers
Name:	AddPrintDrivers
Type	REG_DWORD
Value:	1

I. Do not allow registry editing over the network

Security Impact:	Recommended
Operation Impact:	Evaluate
Implementation:	Simple

The Registry Editor has a function which allows remote access to the Windows NT registry. By default, Windows NT Workstation does not restrict remote access to the registry. To restrict network access to the registry, create the following registry key:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentcontrolSet\Control\SecurePipeServers\winreg

The remote access the registry is defined by the security permissions set on the winreg key.

J. Enable stronger protections on base objects

Security Impact:	Optional
Operation Impact:	High
Implementation:	Simple

In addition to Files, Registry Keys, and Printers, Windows NT has a number of objects that are generally not visible to or known by a typical user. Application programmers learn about these objects in software development kits and use them to exploit the system.

This registry setting informs the Windows NT Session Manager that security on the base system objects should be at C2 security level. The effects of this setting are highly dependent on the environment, so all possible effects that might be experienced cannot be listed. However, the effects will be felt most for users that

redefine system wide resource attributes, such as COM1 or printers. In general this setting will only allow the administration account to administer shared resources.

To enable stronger protection on base objects, add the following value to the registry key.

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Control\SessionManager
Name:	ProtectionMode
Type:	REG_DWORD
Value:	1

The Drive Letters & Printer option of the C2CONFIG utility can also be used to enable stronger protections. See "C2CONFIG utility" on page 37.

K. Wipe the system page file on shutdown

Security Impact:	Optional
Operation Impact:	Medium
Implementation:	Simple

Windows NT uses a page swapping system to expand virtual memory by swapping pages from memory onto disk. Usually this page file is only used by the Windows NT and is well-protected. However, if system can be booted off of another operating system, either by moving the swap disk to another machine or booting off of a separate partition, the swap disk space can be examined. This registry setting ensures that swap file is wiped clean on shutdown.

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Control\SessionManager\Memory Management
Name:	ClearPageFileAtShutdown
Type:	REG_DWORD
Value:	1

This protection only works during a clean shutdown.

L. Enforce strong user passwords

Security Impact:	Necessary
Operation Impact:	Low
Implementation:	Involved

In Service Pack 2 and later a file, Passfilt.dll, is included which can be used enforce these stronger password requirements for users.

- The minimum passwords length is six (6) characters long. This minimum may be increased through the password policy. See "Set password policy" on page 12

- Of the four groups of characters:

  Upper case letters (A thru Z)
  lower case letters (a thru z)
  numbers (0 thru 9)
  non-alphanumeric characters (special characters)

  characters from at least three must be used in passwords.

- Your user name or any part of your full name cannot be used in password.

These requirements are set in the Passfilt.dll file and cannot be changed.
To use Passfilt.dll, setup the following registry key value:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Control\LSA
Name:	Notification Packages
Type:	REG_MULTI_SZ
Value:	Add "PASSFILT" to the string (do not remove existing string).

A second, less restrictive, method is to use the PASSPROP program from the Workstation Resource Kit. The following command will force passwords that contain mixed case or numbers or symbols:

```
c:\> passprop /complex
```

M. Secure EventLog viewing

Security Impact:	Recommended
Operation Impact:	Evaluate
Implementation:	Simple

These registry key settings determine the read access Guests and null accounts have to the Event logs

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Services\EventLog\[LogName]
Name:	RestrictGuestAccess
Type	REG_DWORD
Value:	1

By default the value for the system and application logs keys are set to 0, allowing Guests and null logons to have the ability to view the system and application event logs. By default the value for the security log key is set to 1, Any user with "Manage Audit Logs" user right will be able to view the logs, irrespective of the key values.

The change to these keys take effect on next reboot.

N. Delete unused administrative shares

Security Impact:	Optional
Operation Impact:	Evaluate
Implementation:	Simple

By default Windows NT has hidden shares (sometimes called administrative shares or $ shares). These shares are restricted to administrative functions and will not appear to other computers on the network. However, because they are set by default, it is no secret that they exist and can be attacked from the network.

Although an attacker will need the Administrator password to access the hidden shares, they do represent a vulnerability and can be deleted if they are not needed (no SMB network connections are needed).

To remove the hidden shares, setup the following registry key value:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	CurrentControlSet\Services\LanmanServer\Parameters
Name:	AutoShareWks
Type	REG_DWORD
Value:	0

The administrative shares can also be removed using the Policy Editor by adjusting the Windows NT Network\Sharing\Create hidden drive shares option. See “The Policy Editor” on page 38.

Warning The administrative shares may be required by some Windows NT based network application.

O. Disallow shutdown at the authentication dialog

Security Impact:	Evaluate
Operation Impact:	Evaluate
Implementation:	Simple

By default, a user can shut down Windows NT Workstation without logging on by using the Shutdown in the Logon dialog box. This is not a concern, and, in fact, is a benefit in environments where users can access the computer’s power or reboot switch. However, if the CPU is locked away and managed by a system administrator, not the user, you may want to remove this feature.

To do so create or assign the following Registry key value:

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\Windows NT\Current Version\Winlogon
Name:	ShutdownWithoutLogon
Type:	REG_SZ
Value:	0

The Shutdown Button option of the C2CONFIG utility can also be used to remove the shutdown capability. See “C2CONFIG utility” on page 37.

P. Control access to removable media

Security Impact:	Recommended
Operation Impact:	Medium
Implementation:	Simple

Normally Windows NT allows any program to access files on floppy disks and CDs. Interactive user may want to write sensitive information to these drives and restrict access to other users or program. By setting the following registry keys, the allocation of these drives is restricted to the current interactive process when that process logs on. The drives are deallocated when the user logs off.

Floppy drives may be allocated during logon by creating or assigning the following registry key value:

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\WindowsNT\CurrentVersion\Winlogon
Name:	AllocateFloppies
Type:	REG_SZ
Value:	1

CD-ROMs may be allocated during logon by creating or assigning the following registry key value:

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\WindowsNT\CurrentVersion\Winlogon
Name:	AllocateCDRoms
Type:	REG_SZ
Value:	1

This allocation restriction cannot be enforced by for tape drives.

Any value other than 1 will make the devices available for shared use by all processes on the system.

The settings only take effect subsequent to a logon. Went the values are set, current interactive users will not be effected.

The Removable Media Drives option of the C2CONFIG utility can also be used to secure the drives. See “C2CONFIG utility” on page 37.

Q. Display a legal notice before log on

Security Impact:	Necessary
Operation Impact:	Low
Implementation:	Simple

Before a user logs in, Windows NT can display a message box with a custom caption and text. Set the following registry keys to display the message box:

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	Microsoft\Windows NT\Current Version\Winlogon
Name:	LegalNoticeCaption
Type:	REG_SZ
Value:	Whatever you want for the title of the message box

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	Microsoft\Windows NT\Current Version\Winlogon
Name:	LegalNoticeText
Type:	REG_SZ
Value:	Whatever you want for the text of the message box

Example:

LegalNoticeCaption: WARNING

LegalNoticeText:

To protect the system from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this Automated Information System is prohibited and could be subject to criminal and civil penalties.

The Display Logon Message option of the C2CONFIG utility can also be used to set the legal notice. See "C2CONFIG utility" on page 37.

R. Hide the last user name

Security Impact:	Evaluate
Operation Impact:	Evaluate
Implementation:	Simple

By default, Windows NT leaves the user name of the last user to log on to the computer in the logon dialog box. There are two advantages. First, it is more convenient for the most frequent user to log on. Second, the user may notice if someone else has been logging in, or attempting to log in, to the workstation. However, it also shows anyone who has access to the console your account name. You can prevent Windows NT from displaying the user name from the last logon. This may be important if the computer is located in a highly accessible community area (such as a library). It may also be important if the system administrator often uses the computer and wants to keep the name of the renamed Administrator account secret.

To stop the user name from being displayed in the Logon dialog box, create or assign the following registry key value:

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	\Microsoft\Windows NT\Current Version\Winlogon
Name:	DontDisplayLastUserName
Type:	REG_SZ
Value:	1

The Last Username display option of the C2CONFIG utility can also be used to hide the username. See "C2CONFIG utility" on page 37.

S. Disable caching of logon credentials

Security Impact:	Optional
Operation Impact:	High
Implementation:	Involved

The last logon credentials for a user who logged on interactively to a system, by default, is cached. This is done for system availability and performance reasons.

The credential cache is well protected, but is still available to user with proper access rights. To disable the credential caching set the following registry key:

Hive:	HKEY_LOCAL_MACHINE\SOFTWARE
Key:	Microsoft\Windows NT\CurrentVersion\Winlogon
Name:	CachedLogonsCount
Type:	REG_DWORD
Value:	0

X. Resource Kit tools

The NT Workstation include several utilities that may be of use in securing and monitoring the security of a system

A. Summary of security related tools

AUDITCAT.HLP	A help package for the Events Viewer that gives all the event codes and what they mean.
AUTOEXNT.EXE	A utility used to run batch jobs at system startup time without having to log in as a user.
C2CONFIG.EXE	A utility that helps examine and implement C2 security safeguards.
DUMPEL.EXE	A DOS command line utility which will dump the contents of the event logs in ASCII form.
LOGEVENT.EXE	A DOS command line utility which can be used to send text strings to the event log as event messages.
NETWATCH	A program that will pop up a window showing which remote machines are accessing shares. It also gives the ability to disconnect remote machines from share use.
PASSPROP	A DOS command line utility for modifying the registry to enforce strong password rules or to lock out the Administrator account from remote access.
PERMCOPY.EXE	A DOS command line utility for copying share permissions from one share to another.
PERMS.EXE	A DOS command line utility which can be used to list a specific user's access permissions to files.
POLEDIT.EXE	Policy Editor: a program for setting up specific criteria (policy) for a user's account.
SCOPY.EXE	A DOS copy command which will copy files and retain all their original security settings (the normal COPY command changes ownership
SECEDIT.EXE	A DOS command line utility which can be used to edit permissions for an active process.
SHOWACLS.EXE	A DOS command line utility for showing the access controls attached to a file.
SU.EXE	A DOS command line utility which can be used to "switch" to another user account.
WINEXIT	A screen saver that logs the user out after a predetermined time.

B. C2CONFIG utility

Many functions that are described elsewhere in this document can be implemented more safely and quickly by using the C2CONFIG.EXE program.

Start the C2CONFIG window from the DOS prompt:

```
c:\> C2CONFIG
```

Choose the appropriate option.

To get more information about any of the options:

Single click (highlight) the option.
Pulldown the Help menu.
Select On Selected Item.

C. The Policy Editor

Many functions that are described elsewhere in this document can be implemented more safely and quickly by using the Policy Editor. For instance, to change some registry settings, do the following:

Start the Policy Editor from the DOS prompt:

```
C:\> poledit
```

When the Policy Editor window opens:

Pulldown the File menu and select Open Registry.
Double Click on Local Computer.
Adjust any parameter as needed.
Click the OK button.
Pulldown the File menu and select Save.

D. Enable blocking of the Administrator account

Security Impact:	Optional
Operation Impact:	Low
Implementation:	Very Easy

If network access to the Administrator account cannot be disabled (see “Disable network logon privileges for the Administration account” on page 4), the PASSPROP program from the Resource Kit can be used to cause the Administrator account to lockout after multiple failed login attempts.

PASSPROP only locks network access. The Administrator account is always accessible from the console.

To get help on passprop, use the DOS prompt command:

```
C:\> passprop ?
```

To lock out the Administrator account use the command:

```
C:\> passprop /adminlockout
```

The Account Lockout Policy must be set for the PASSPROP lockout feature to take effect. See “

For stronger enforcement of passwords, see “Enforce strong user passwords” on page 31

Set account lockout policy” on page 12.

E. Use the auto-logoff screensaver

Security Impact:	Recommended
Operation Impact:	High
Implementation:	Simple

The workstation can be set to automatically log the user off if it is not used for a set period of time by using the screensaver, WINEXIT.SCR, from the Resource Kit.

Move the file WINEXE.SCR from the Resource Kit into the %SYSROOT%\System32 directory.
Right click on a "blank" area of the screen and select Properties or select Display from the Control Panel.
Select the ScreenSaver tab on the Properties popup window.
Select the Logoff Screen Saver.
Enter the desired wait time.
Adjust the settings as needed.

Note that password protection on the screen saver will still work if password protection is selected (see "Use the locking screensaver" on page 17)

For users to use WINEXIT they must have Set Value and Create Subkey permissions on the registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\Current Version

Warning When the screensaver forces the logoff, any interactive process that is running will be killed. Running programs that take several hours to complete may become impossible.

F. Remove the Everyone account

Security Impact:	Optional
Operation Impact:	Evaluate
Implementation:	Involved

If users are granted access to files and registry keys through specific local groups, rather than the generic Everyone account, the Everyone account is not needed. Removing the Everyone group from the system can significantly reduce the effectiveness attacks. To remove the Everyone group, first set all directory, file, and registry key permissions so that they do not rely on the Everyone group for proper access. Second, make a backup of the registry using the REGBACK.EXE utility from the Resource Kit. Finally, run REGSEC.EXE from the Resource Kit.

Warning **1)** The Everyone group is often relied upon by the standard Windows NT system to allow users to read critical files and registry keys. Make sure valid users have the same access as Everyone before removing the Everyone account. This can be done by creating a special universal group (e.g. ALLUSERS) and adding all valid users to this group. Substitute ALLUSERS for Everyone in the permissions for files, registry keys, and other resources.

2) The REGSEC.EXE program does not have an analogous operation or program for restoring the Everyone group. Once the Everyone group has been removed from the registry, it is gone. That is why it is extremely important to use REGBACK.EXE to make a copy of the registry before REGSEC.EXE is used.

If removing the Everyone group breaks critical functions, the easiest way to restore will be to restore the back up registry.

XI. Appendix

A. Hot Fixes for Service Pack 3 as of April 1998

Hot Fix	Date of Fix	MS KB article	Description
oob-fix		Q143478	Superseded by teardrop2-fix
java-fix		Q168748	Superseded by getadmin-fix
dblclick-fix		Q170510	Superseded by getadmin-fix
icmp-fix		Q154174	Superseded by teardrop2-fix
land-fix		Q165005	Superseded by teardrop2.fix
mdl-fix		Q179433	Superseded by getadmin-fix
asp-fix	05/28/97	Q165335	If you are running Active Server Pages version 1.0b on Microsoft Internet Information Server (IIS) version 3.0, you may experience performance problems. It may take a long time for you to notice these performance problems, depending on how often the Active Server Pages are accessed.
dns-fix	06/09/97	Q142047 Q154984 Q154985 Q167629 Q169461	The Domain Name Services (DNS) has problems including a possible denial of service attack.
iis-fix	06/20/97	Q143484	The Internet Information Server service stops when it receives a CGI request from a browser that contains between 4 and 8 kilobytes of data in the URL.
lsa-fix	06/25/97	Q154087	While running Windows NT, you may receive an Access Violation error message in Lsass.exe. After this error occurs, you cannot logon locally and the administrative tools that rely on LSA/LSARPC (such as Event Viewer and Server Manager) do not function.
lm-fix	07/11/97	Q147706	To allow access to servers that only support LM authentication, Windows NT clients currently send both LanManager and Windows NT authentication types. Microsoft developed a patch that supports a new registry key that allows clients to be configured to send only Windows NT authentication.
zip-fix	07/14/97	Q154094	Windows NT cannot access the disk in the ATAPI version of an Iomega Zip drive
roll-up	11/24/97	Q147222	An Access Violation occurs in Windows NT Explorer (Explorer.exe) and other applications while running Microsoft Transaction Server (MTS).

getadmin-fix	07/15/97	Q146965 Q168748 Q170510	A utility, Getadmin.exe, is being circulated on the Internet that grants normal users administrative rights by adding them to the Administrators group. This utility can be run from any user context except Guest and grants a local user account administrative rights. Also, Internet Explorer version 3.02 may hang when connecting to a Web link that contains a Java application after you have installed Windows NT version 4.0 Service Pack 3. Also, Double-clicking the mouse in your application behaves as if you clicked the mouse button once.
winsupd-fix	08/07/97	Q155701	Invalid UDP frames directed to any computer running WINS raises an exception in WINS causing it to terminate silently.
ndis-fix	08/08/97	Q156655	When intermediate (layered) NDIS miniport drivers are in use on Windows NT 4.0, you may experience one or both of the following: • A memory leak • A blue-screen STOP error message with parameters that indicate the bad instruction is in the NDIS.SYS driver.
scsi-fix	09/05/97	Q171295	With the FirstWatch program, transition failures have been observed that require the use of CLARION's Trespass utility.
2gcrash	11/01/97	Q173277	In systems where RAM exceeds 1.7 GB, Memory.dmp files are not generated.
simptcp-fix	11/01/97	Q154460	A malicious denial of service attack may be mounted against Windows NT computers with the Simple TCP/IP Services installed. The attack consists of a flood of UDP datagrams sent to the subnet broadcast address with the destination port set to 19 and a spoofed source IP address.
ide-fix	11/18/97	Q153296	Write cache on IDE/ATAPI Disks is not flushed on shut down. You may experience one of the following problems: • CHKDSK runs as your computer starts and reports a dirty volume. • A blue screen appears and displays the following message: STOP 0x0000007B (parameter, parameter, parameter, parameter) INACCESSIBLE_BOOT_DEVICE
wan-fix	11/20/97	Q163251	You may experience a STOP 0x0000000A on a Windows NT computer when copying files via RAS over a SLIP (Serial Line Interface Protocol) connection.

pent-fix	12/11/97	Q163852	When an Intel processor receives a specific invalid instruction, your computer may stop responding (hang). Your computer must be turned off and restarted to return to normal operation.
joystick-fix	12/11/97	Q177668	The value of the calibration bar may not change when you attempt to calibrate foot pedals attached to the joystick game port.
SAG-fix	12/11/97	Q177471	A Windows NT client or server that receives EBCDIC characters from an IBM-compatible computer does not convert properly from EBCDIC character codes to ANSI character codes.
iis4-fix	12/12/97	Q169274	In TCP/IP, timewait state queue management had a problem that caused time wait states to exceed four minutes under stress.
pptp-fix	01/08/98	Q179107	A STOP 0x0000000A in Raspptpe.sys on PPTP server running Windows NT while PPTP clients are connecting.
teardrop2-fix	01/09/98	Q143478 Q154174 Q165005 Q179129	Windows NT may stop responding (hang) after receiving a number of deliberately corrupted UDP or ICMP packets.
tapi21-fix	01/12/98	Q179187	Problems using TAPI 2.1
pcm-fix	02/11/98	Q180532	The Xircom CBE-10/100BTX PC Card may fail to function.
srv-fix	02/12/98	Q180963	During the processing of a Server Message Block (SMB) logon request, memory corruption occurs causing a system reboot or system hang.
y2k-fix	03/27/98	Q175093 Q180122 Q183123 Q183125	Fixes multiple year 2000 problems
euro-fix	04/08/98	Q182005	Add a euro currency symbol to the Windows NT symbol set.
atapi-fix	04/16/98	Q183654	Corrects incorrect reporting of 10 gigabyte drive
nbtfix	04/22/98	Q178205	Corrects delays in using LMHOSTS file to resolve addresses.

B. Suggested workstation user rights

User Right	Groups assigned this right by default
Act as part of the operating system (SeTcbPrivilege) Processes may perform as a secure, trusted part of the operating system. Some of the Windows NT subsystems are granted this right.	(None)
Add workstations to the domain (SeMachineAccountPrivilege) User may add workstations to a particular domain. Since this right is meaningful only on domain controllers, it is normally not used on Workstations.	(None)
Back up files and directories (SeBackupPrivilege) User may supersede file and directory permissions for back up purposes.	Administrators, Backup Operators, Power Users
Bypass traverse checking (SeChangeNotifyPrivilege) User may change directories and access files and subdirectories irrespective of access to parent directories.	Everyone
Change the system time (SeSystemTimePrivilege) User may set the internal clock of the computer.	Administrators, Power Users
Create a pagefile (SeCreatePagefilePrivilege) User may create new pagefiles for virtual memory swapping.	Administrators
Create a token object (SeCreateTokenPrivilege) Process may create access tokens. Normally only the Local Security Authority may create access tokens.	(None)
Create permanent shared objects (SeCreatePermanentPrivilege) User may create special permanent objects (such as \\Device).	(None)
Debug programs (SeDebugPrivilege) Various low-level objects such as threads may be debugged.	Administrators
Force shutdown from a remote system (SeRemoteShutdownPrivilege) A Windows NT system may be remotely shutdown over a network.	Administrators, Power Users
Generate security audits (SeAuditPrivilege) Security audit log entries may generated.	(None)
Increase quotas (SeIncreaseQuotaPrivilege) Current versions of Windows NT do not use this right. It has no effect.	Administrators
Increase scheduling priority (SeIncreaseBasePriorityPrivilege) User may boost the execution priority of a process.	Administrators

Load and unload device drivers (SeLoadDriverPrivilege) Allows a user to install and remove device drivers.	Administrators
Lock pages in memory (SeLockMemoryPrivilege) Allows a user to lock pages in memory so they cannot be paged out to a backing store such as Pagefile.sys.	(None)
Log on as a batch job Nothing. This right has no effect in current versions of Windows NT.	(None)
Log on as a service Allows a process to register with the system as a service.	(None)
Manage auditing and security log (SeSecurityPrivilege) Allows a user to specify what types of resource access (such as file access) are to be audited, and to view and clear the security log. Note that this right does not allow a user to set system auditing policy using the Audit command in the Policy menu of User Manager. Also, members of the Administrators group always have the ability to view and clear the security log.	Administrators
Modify firmware environment variables (SeSystemEnvironmentPrivilege) Allows a user to modify system environment variables stored in nonvolatile RAM on systems that support this type of configuration.	Administrators
Profile single process (SeProfSingleProcess) Allows a user to perform profiling (performance sampling) on a process.	Administrators
Profile system performance (SeSystemProfilePrivilege) Allows a user to perform profiling (performance sampling) on the system.	Administrators
Replace a process-level token (SeAssignPrimaryTokenPrivilege) Allows a user to modify a process's security access token. This is a powerful right used only by the system.	(None)
Restore files and directories (SeRestorePrivilege) Allows a user to restore backed-up files and directories. This right supersedes file and directory permissions	Administrators, Backup Operators
Take ownership of files or other objects (SeTakeOwnershipPrivilege) Allows a user to take ownership of files, directories, printers, and other objects on the computer. This right supersedes permissions protecting objects.	Administrators

C. Default services

Service	Description
Alerter	Forwards alerts generated on local machines to remote computers or usernames. See "Remove Alerter and Messenger services" on page 17.
ClipBook Server	Supports viewing of Clipboard from remote workstations.
Computer Browser	Browses network for other NetBios services in the Domain. If the Browser is stopped, users can still access services by typing the explicit computer name or using the Find command.
Directory Replicator	Use to replicate directories. Not needed if replication is not used.
EventLog	Used by Event Logger. Cannot be stopped or paused.
Messenger	Sends and receives messages sent by administrators. See "Remove Alerter and Messenger services" on page 17.
Net Logon	Supports pass-through authentication (single sign-in) in a domain.
Network DDE	Provides a network transport for Dynamic Data Exchange.
NT LM Security Support Provider	Provides Remote Procedure Call security that uses transports other than named pipes.
Remote Procedure Call (RPC) Locator	Allows applications to use the RPC service used by many network applications.
Remote Procedure Call (RPC) Service	The RPC service. This service cannot be stopped.
Schedule	Required to run the AT command.
Server	Allows Windows NT to share resources using the SMB service (such as Shares).
Spooler	Provides print spooling.
TCP/IP NetBIOS Helper	Provides NetBIOS over TCP/IP transport.
UPS	Used for connection to Uninterruptable Power Supplies.
Workstation	Allows access to network Workgroup resources and allows logging into a domain.

D. Recommended folder and file permissions

In the following tables %SYSTEMROOT% refers to the directory where Windows NT has been installed. Usually %SYSROOT% is C:\WINNT

	Permissions
%SYSROOT% and *all subdirectories* under it.	Administrators: Full Control Creator Owner: Full Control Everyone: Read System: Full Control

Now, within the %SYSROOT% tree, apply the following exceptions to the general security:

Directory	Permissions
%SYSROOT%\REPAIR	no access
%SYSROOT%\SYSTEM32\CONFIG	Administrators: Full Control Creator Owner: Full Control Everyone: List System: Full Control
%SYSROOT%\SYSTEM32\SPOOL	Administrators: Full Control Creator Owner: Full Control Everyone: Read POWER USERS: Change System: Full Control
%SYSROOT%\COOKIES %SYSROOT%\FORMS %SYSROOT%\HISTORY %SYSROOT%\OCCACHE %SYSROOT%\PROFILES %SYSROOT%\SENDTO %SYSROOT%\Temporary Internet Files	Administrators: Full Control Creator Owner: Full Control Everyone: Special Directory Access – Read, Write and Execute, Special File Access – None System : Full Control

Warning The directory %SYSROOT%\REPAIR is used to create an Emergency Repair Disk (ERD). When an ERD is being created, the permissions on this file must be changed to Administrators: Full Control.

Several critical operating system files exist in the root directory of the system partition on Intel 80486 and Pentium-based systems. These are hidden files. To view the files:

> Pulldown the View menu and select By File Type.
> Check mark the Show Hidden/System Files box.

Assign the following permissions to these files:

File	C2-Level Permissions
\Boot.ini, \Ntdetect.com, \Ntldr	Administrators: Full Control System: Full Control
\Autoexec.bat, \Config.sys	Everybody: Read Administrators: Full Control System: Full Control
\TEMP directory	Administrators: Full Control System: Full Control Creator Owner: Full Control Everyone: Special Directory Access – Read, Write and Execute, Special File Access – None

It is also highly advisable that Administrators manually scan the permissions on other directories, such as Program Files, to ensures that they are appropriately secured for various user accesses in their environment.

Utilities that may help to scan and change permissions are the CACLS command (see Appendix F "Using CACLS" on page 49) and the PERMS and SHOWACLS utilities from the Workstation Resource Kit.

E. Highly secure registry protections

For each of the keys listed below, restrict the Everyone group to QueryValue, Enumerate Subkeys, Notify and Read Control.

In the HKEY_LOCAL_MACHINE:

\Software

> Note: This change is recommended. It locks the system in terms of who can install software. Note that it is **not** recommended that the entire subtree be locked using this setting because that can render certain software unusable

\Software\Microsoft\RPC (and its subkeys)

> This locks the RPC services.

\Software\Microsoft\Windows NT\ CurrentVersion
\Software\Microsoft\Windows NT\ CurrentVersion\Profile List
\Software\Microsoft\Windows NT\ CurrentVersion\AeDebug
\Software\Microsoft\Windows NT\ CurrentVersion\Compatibility
\Software\Microsoft\Windows NT\ CurrentVersion\Drivers
\Software\Microsoft\Windows NT\ CurrentVersion\Embedding
\Software\Microsoft\Windows NT\ CurrentVersion\Fonts
\Software\Microsoft\Windows NT\ CurrentVersion\FontSubstitutes
\Software\Microsoft\Windows NT\ CurrentVersion\Font Drivers
\Software\Microsoft\Windows NT\ CurrentVersion\Font Mapper
\Software\Microsoft\Windows NT\ CurrentVersion\Font Cache
\Software\Microsoft\Windows NT\ CurrentVersion\GRE_Initialize
\Software\Microsoft\Windows NT\ CurrentVersion\MCI
\Software\Microsoft\Windows NT\ CurrentVersion\MCI Extensions
\Software\Microsoft\Windows NT\ CurrentVersion\PerfLib

> Consider removing Everyone:Read access on this key. This allows remote users to see performance data on the machine. Instead you could give INTERACTIVE:Read Access which will allow only interactively logged on user access to this key, besides Administrators and System.

\Software\Microsoft\Windows NT\ CurrentVersion\Port (and all subkeys)
\Software\Microsoft\Windows NT\ CurrentVersion\Type1 Installer
\Software\Microsoft\Windows NT\ CurrentVersion\WOW (and all subkeys)

\Software\Microsoft\Windows NT\ CurrentVersion\Windows3.1MigrationStatus (and all subkeys)

\System\CurrentControlSet\Services\LanmanServer\Shares

\System\CurrentControlSet\Services\UPS

> Note that besides setting security on this key, it is also required that the command file (if any) associated with the UPS service is appropriately secured, allowing Administrators: Full Control, System: Full Control only.

\Software\Microsoft\Windows\CurrentVersion\Run

\Software\Microsoft\Windows\CurrentVersion\RunOnce

\Software\Microsoft\Windows\CurrentVersion\Uninstall

In the HKEY_CLASSES_ROOT:

\HKEY_CLASSES_ROOT (and all subkeys)

In the HKEY_USERS on Local Machine dialog:

\.DEFAULT

Some paths that need to be accessible by non-administrators are specified in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Contro\SecurePipeServers\winreg\AllowedPaths key.

F. Using CACLS

CACLS is a command for viewing and changing Access Control Lists (ACLS) from the DOS prompt. One advantage of this command is the ability to quickly list out the ACLS for numerous files with a single command (as opposed to point and click for each individual file). Obviously, as the ACLS for hundreds of files are spilling out, it is advantageous to redirect the output to a file for later examination:

```
C:\> cacls * > fileacls.txt
```

Unfortunately, Service Pak 2 and Service Pak 3 “break” the cacls command by rendering redirection of the output impossible. The fix recommended by Microsoft is to recover the original cacls.exe off of the Windows NT CD.

The file on the CD is a compressed file called cacls.ex_. Use the utility EXPNDW32.EXE from the Resource Kit to expand cacls.ex_ into the usable program calcs.exe.

G. Creating simultaneous logins

While adjusting security parameters it is often valuable to check the effects of security changes on “unprivileged” accounts (accounts with minimal rights). Since the adjustment of most security parameters require administrative rights, checking the effects of each change means logging out of the administrative account and logging into an unprivileged account. This is a time consuming and irritating task, even on “fast” machines.

The following is a method of having two accounts logged in from a single terminal simultaneously using the programs DESKTOPS.EXE and SU.EXE from the Resource Kit.

Log in as Administrator.
Run the Resource Kit Desktops command:

```
C:\> desktops
```

Right click on a “blank” area of the desktops menu bar (avoiding the desktop buttons) to bring up a desktops pulldown.
Select Properties.
Under the Startup Shell tab, choose No Desktop Shell.
Under the Options tab, choose Save Settings On Exit.
Click OK.
Right click on the “blank” area and select Exit from the pulldown.
Run Desktops again.
Click the Desktop #2 button. An empty Desktop should appear.
Right click on the “blank” area and select run.
Enter the following command in the command window where “newuser” is a valid account name:

```
su newuser
```

A DOS command window will pop up with a password prompt.
Enter newuser’s password.
Another DOS command window will pop up. Enter the following commands:

```
C:\> set userprofile=c:\winnt\profiles\newuser
C:\> explorer
```

The desktop for the newuser account should appear.
DO NOT close the DOS command windows! If these windows are closed the desktop will remain, but programs will not run.

Now the switch between the Administration account and the newuser account can be made simply by switching desktops.

Warning: This is not a flawless solution. The second desktop may start acting “flaky” and may not run all programs correctly. This method is not recommended for everyday use, but it seems to work well for testing access permission, desktop and profile changes, and registry changes.