Global Information Assurance Certification Paper

Essential Steps for Securing a Windows NT 4 Server

Justin Saxinger

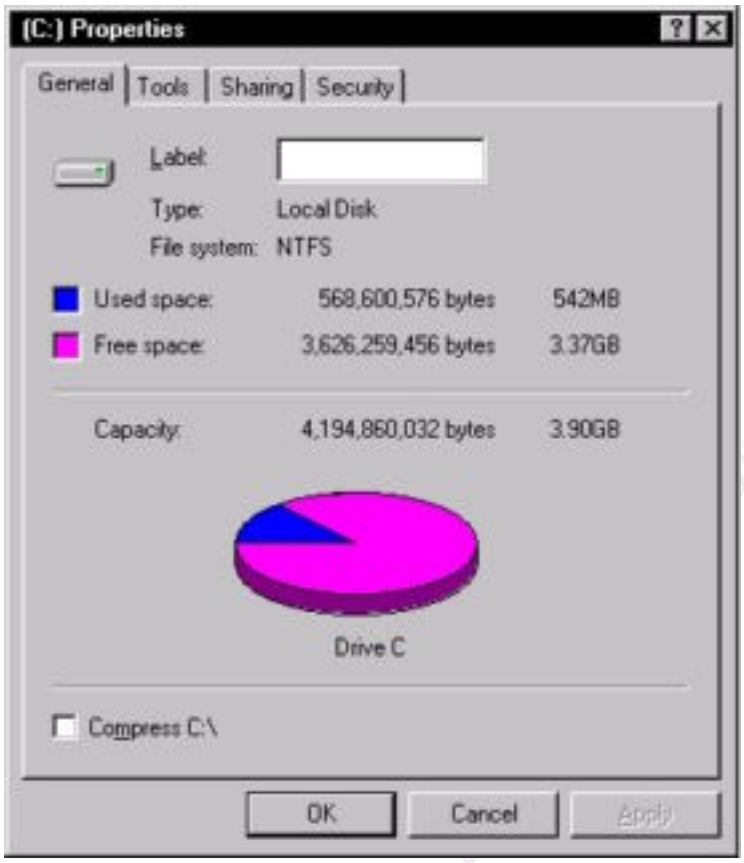
While Windows NT does offer some security out of the box, for any network that requires more than minimal protection, steps must be made to defend the server from attacks. The following steps show the most important and essential procedures in properly securing a Windows NT server that is running as either a domain controller or a stand-alone server used by both Windows and Macintosh clients. First the server's hardware and file system must be secured. Then the operating system must be updated and configured to remove unnecessary components. Access to the server must be protected by modifying user account policies and by securing file and share permissions. Finally, the server should be protected against attacks by using anti-virus software and through the use of thorough auditing procedures.

Hardware Security

The initial step in defending your server is to protect the machine itself. Make sure the computer is in a locked and secure location where only the server operators and other authorized users have access. The case for the computer should also be locked to hinder tampering. In case an unauthorized user is able to gain physical access to the server, it should be protected against being started with another operating system that may compromise security. A person could start with an MS-DOS diskette containing NTFSDOS and be able to bypass NT security. Disable the ability to boot from any device other the hard drive in the BIOS. Once the BIOS has been configured it must be locked with a password to prevent changes.

File Format

Most of NT's security features discussed later rely on the type of file system used on the server. The NTFS file system must be used on all volumes. NTFS is necessary for assigning file and folder permissions and for the ability to audit access to files and folders. Check the existing file format by right-clicking on a volume and selecting properties.

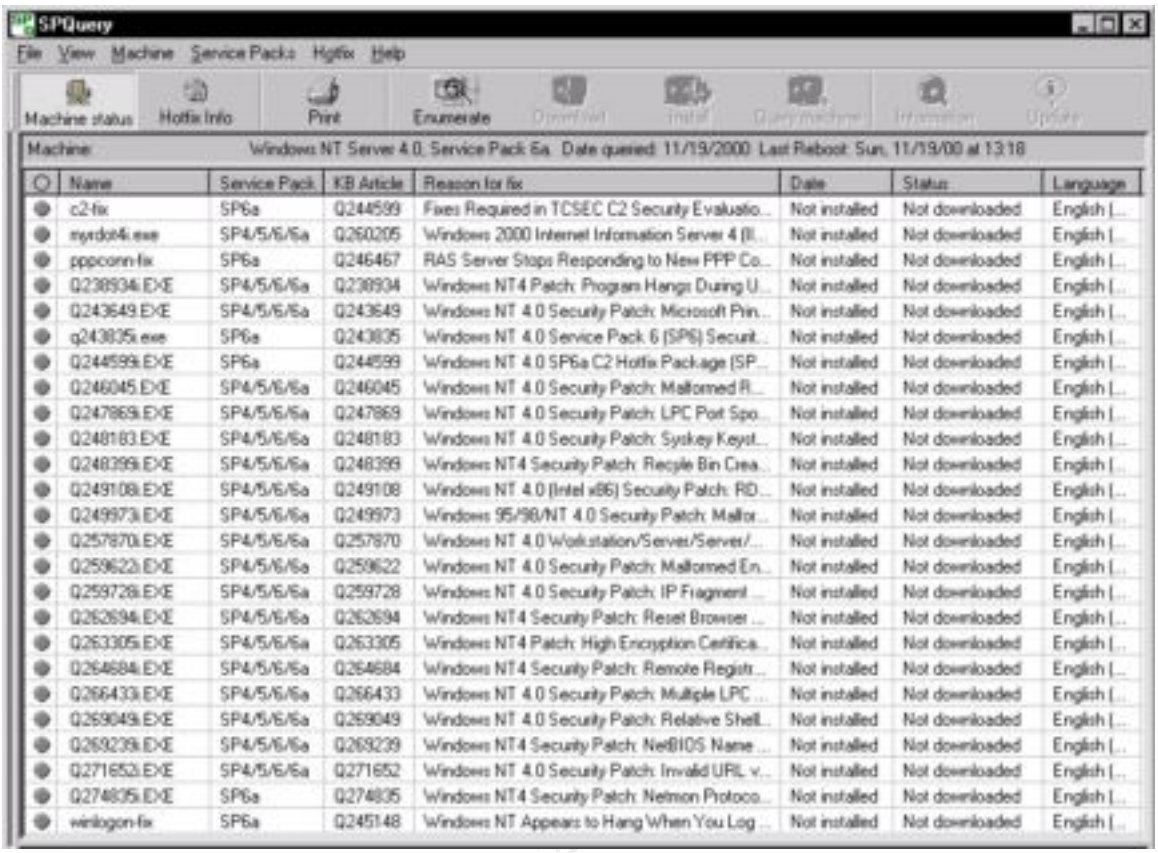


If any volumes are using FAT, use the convert command to change to NTFS. Go to the command prompt and type 'convert *drive letter*: /fs:ntfs'. If the volume cannot be converted while the server is running the conversion will occur during the next reboot. After running the convert command the NTFS file permissions will be set to Everyone – Full Control, leaving the server wide open. At the very least, set the permissions to the NT default values using fixacls.exe. The utility is available on the NT 4 Resource Kit.

Update the Operating System

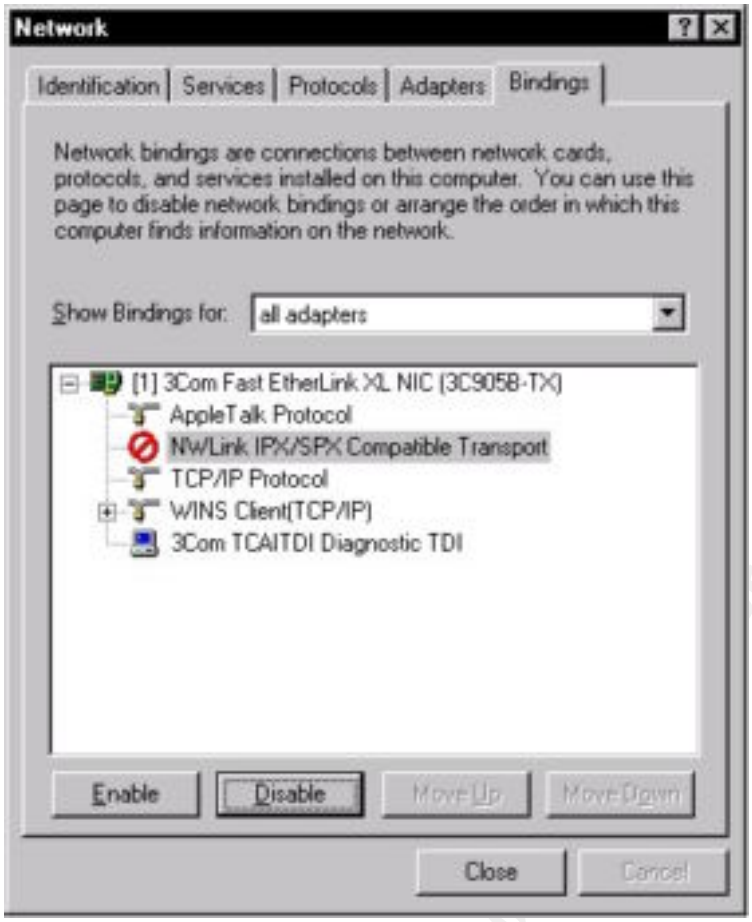
Discovering new bugs in the operating system is an ongoing process. While most bugs are of minor importance, many are major vulnerabilities in the security of the OS and are easily exploitable. It is vital to continually update the OS by installing the latest service packs. You can check the currently installed service pack by typing 'winver' at the run command.

The current service pack at this date is 6a. Microsoft's Service Pack Information page at http://www.microsoft.com/technet/security/srvpckin.asp keeps an up to date list of the current service pack versions. If the server has not been updated, the latest service pack can be downloaded at http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/allSP6.asp. In addition to the current service pack, the latest hot fixes must also be applied. Microsoft frequently releases these patches in response to new vulnerabilities discovered in between the major service pack releases. The latest hot fixes can be downloaded at http://www.microsoft.com/ntserver/nts/downloads/. A third party tool such as St. Bernard Software's SPQuery will allow you to easily view your currently installed hot fixes and to centrally manage distribution.



Remove Unnecessary Components

A basic concept in computer security is that the more the system is running, the more there is to attack. Simply by removing unnecessary components, the number of vulnerabilities on a system can be greatly reduced. First unbind any protocols that are not necessary such as IPX/SPX or NetBIOS to remove any exposures associated with those protocols.



Most applications do not require the OS/2 or POSIX subsystems. If the server does not require these subsystems, they should be removed. Delete the \winnt\system32\os2 directory and its subdirectories. Then you must make the following changes to the registry:

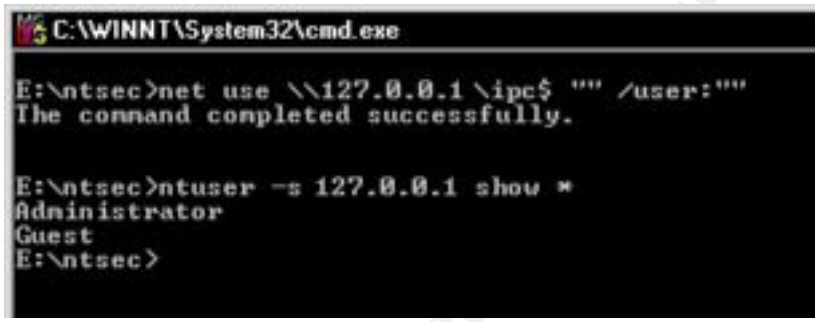
- *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT:* delete all sub keys
- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment*: delete the Os2LibPath value.
- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems*: delete the values for Optional
- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems*: delete the Posix and OS/2 keys

Some services can also add vulnerabilities to NT. The Messenger service can be used to expose the administrator's username. The Scheduler service can allow users to run applications that would normally exceed their security access. All services not necessary for the server to function should be disabled.

Account Security

Once the major vulnerabilities in the operating system have been removed, the next phase is to ensure that the user accounts are secured. The first step in setting proper account security is to protect the built-in accounts. The Administrator account should be renamed and disguised as a regular user account. Next copy this account and give the copy the name Administrator and remove this account from all groups and make sure it has no privileges on the network. This false account can server has a honeypot against attackers. To prevent an attacker from continually trying to gain the Administrator password, passprop.exe should be used to enable lockout of the Administrator account. The utility can be installed from the NT 4 Resource Kit. Go to the command line and type 'passprop /adminlockout'. Finally, the strongest password possible should be used for the Administrator account. The password should be at least 9 characters long, use random characters and numbers, and use at least one extended ASCII character created by using the Alt key and a 3-digit key from the numeric keypad. The second built-in account, Guest, should be disabled.

Any remote user can get a list of all user accounts by exploiting the null user session and using a utility such as Pedestal Software's NTUSER application.



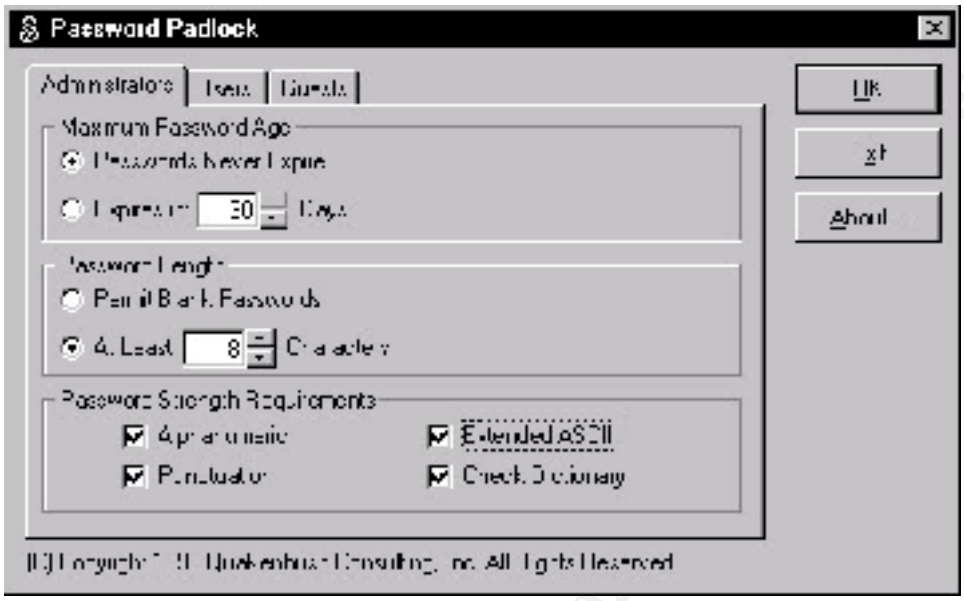
To block a null session from being able to list users on the server make the following change to the registry:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA
Value Name: *RestrictAnonymous*
Value Type: *REG_DWORD*
Value Data: *1*

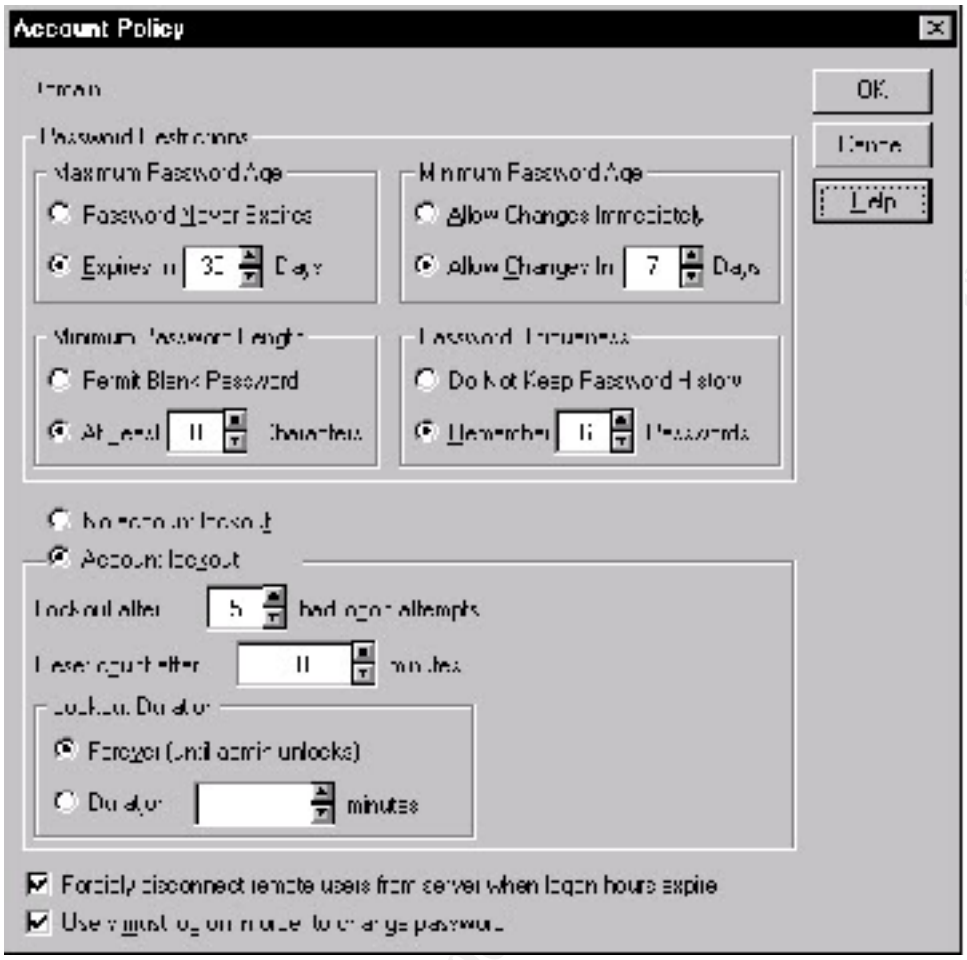
The next step in protecting user accounts is to ensure they all use sufficiently secure passwords. Passwords such as usernames or simple words that can be found in the dictionary are easily guessed. Microsoft's PasswordFilter can be used to enforce password rules. When used, passwords must be at least 6 characters long, they cannot contain the username or any portion of the user's full name, and must contain 3 of the 4 following classes of characters: upper case letters, lower case letters, numbers, and non-alphanumeric characters such as punctuation symbols. To enable the PasswordFilter, make the following change to the registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages. Add the line passfilt.dll to the multiple string value.

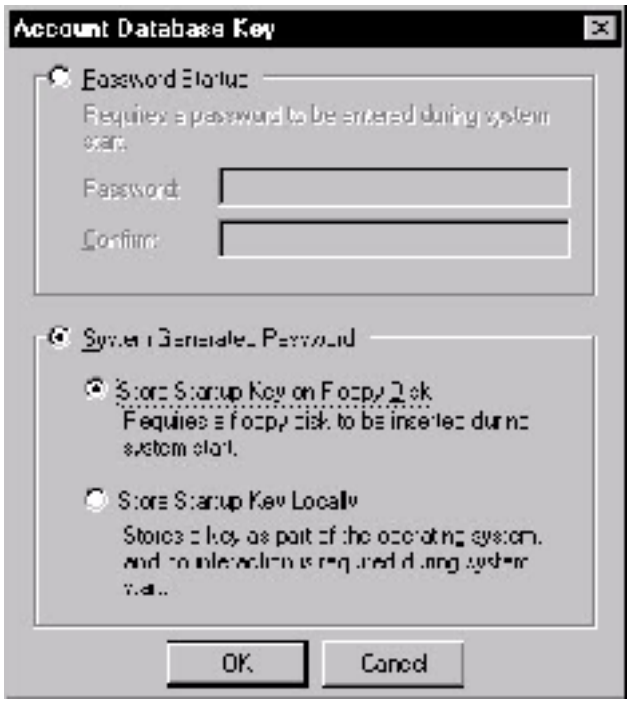
In addition to Microsoft's PasswordFilter, third party utilities are available such as Quakenbush's Password PadLock. These utilities offer more control over password policies.



Next use the Account Policy dialog in User Manager to set additional configurations for account password and lockout policies. The minimum password length should be at least 8 characters. Note that users connecting to the server from Macintosh clients cannot use passwords longer than 8 characters. The minimum password age should be between 1 and 7 days. The maximum password age should be no more than 42 days. The number of remembered passwords should be at least 8. Accounts should be locked out after 3-5 failed attempts, the count should reset after no less than 30 minutes, and the lockout should be set to Forever until the administrator unlocks it.



The final step in securing the accounts is to secure the SAM database itself. Since utilities such as L0phtCrack can extract passwords from the database, it is important to encrypt the data. By using the syskey.exe utility, the SAM can be encrypted with a 128-bit random key. The password encryption key is protected by the System Key. There are three ways to manage the System Key. The first option is to use a computer generated random key and store the key on the server using Microsoft's "complex obfuscation algorithm." This will allow for the server to be restarted unattended, but does not protect the key as well as the other two methods. The random key can also be stored on a floppy disk. The disk can then be physically secured, but the disk is required for the operating system to start. The third option is to use a password to derive the System Key. The password must be entered when the server is started.



File and Share Permissions

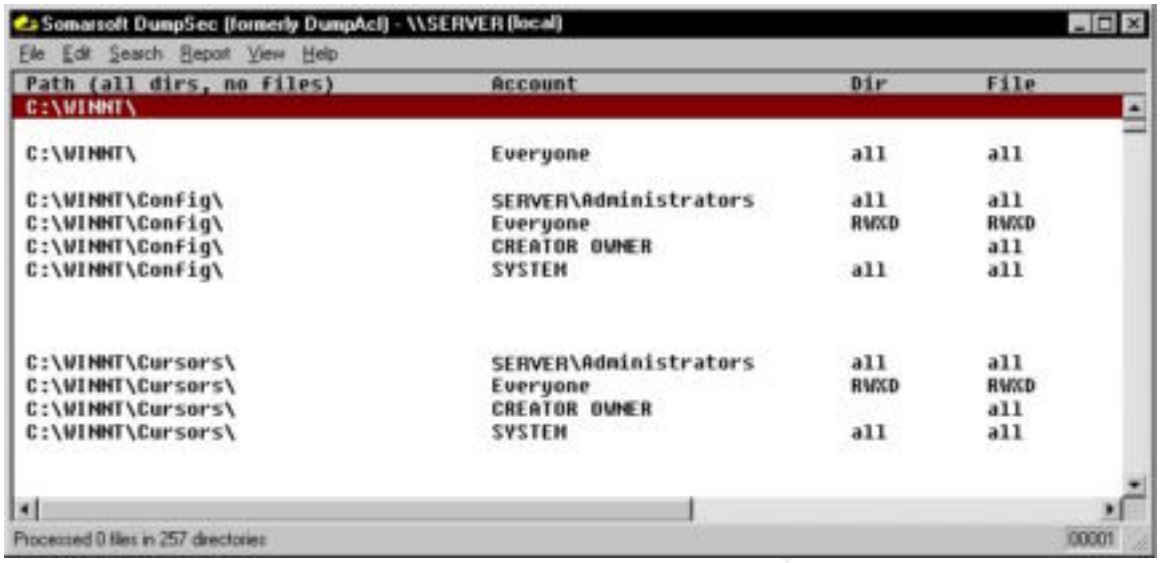
Once the user accounts have been secured, file and share permissions must be checked for vulnerabilities. To prevent unauthorized users from listing sharenames residing on your server you should block null session users. Create the following registry value:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA
Value Name: *RestrictAnonymous*
Value Type: *REG_DWORD*
Value Data: *1*

To block null session users from not only listing shares but also accessing the shares create the following registry value:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters
Value Name: *RestrictNullSessAccess*
Value Type: *REG_DWORD*
Value Data: *1*

The NTFS and share permissions on the system volume should be restricted as much as possible. To view the current permissions you can view each folder's properties individually with Windows Explorer. A much quicker and easier method would be to use a third party tool. With Somarsoft's Dumpsec you can view the permissions for the entire volume within one interface.



While the default NT permissions do provide an adequate level of security for some systems, they are more open than what is needed for a secure server. If you have just installed NT or have run the fixacls.exe utility, you should change the NTFS permissions to further restrict access. The following table lists Trusted Systems Services, Inc.'s recommended permissions for NT.

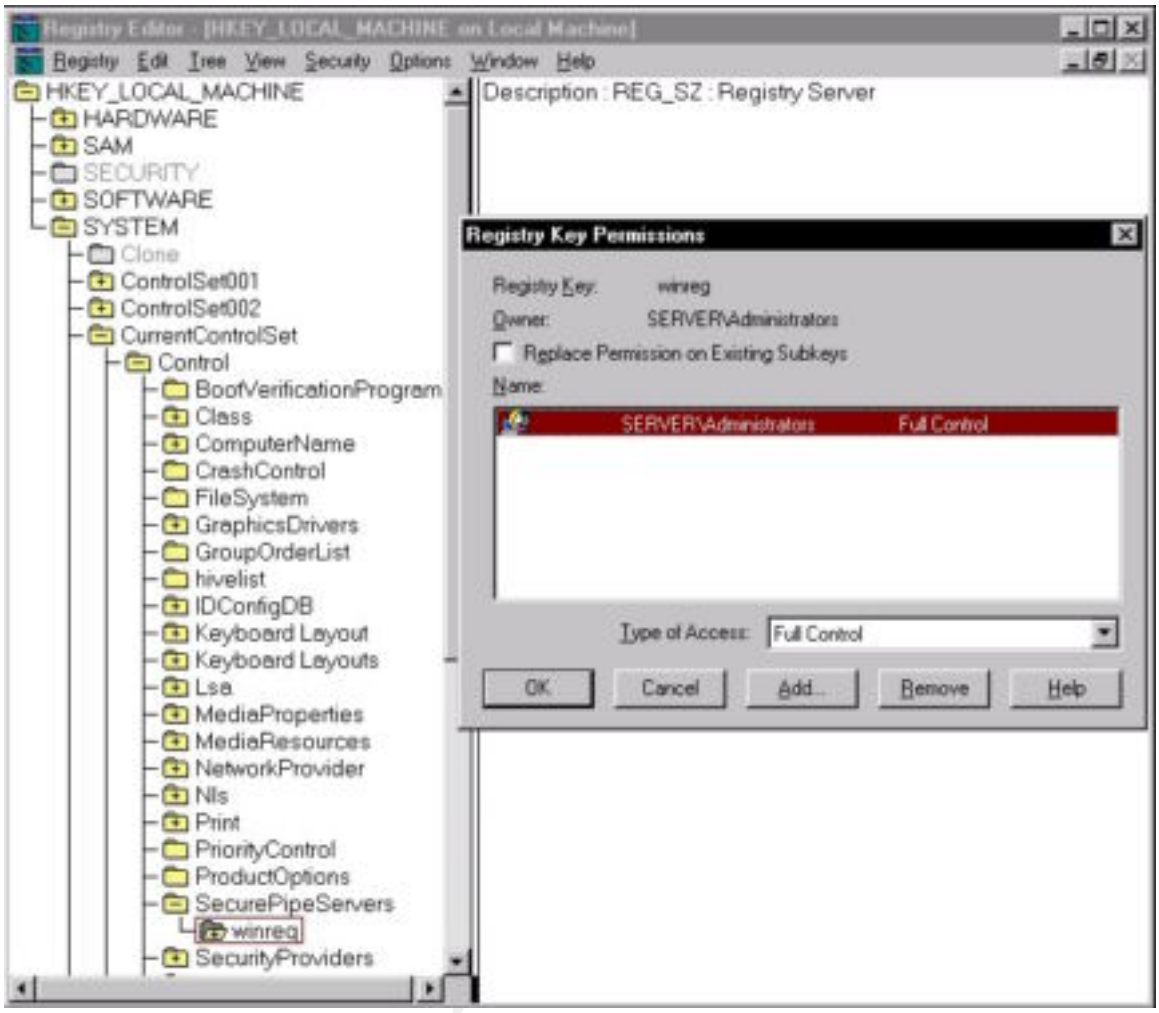
Directory or file	Suggested Max Permissions
C:\	Installers: Change Everyone: Read Server Operators: Change Power Users: Add
files	Installers: Change Everyone: Read Server Operators: Change
IO.SYS, MSDOS.SYS	Installers: Change Everyone: Read Server Operators: Change
BOOT.INI, NTDETECT.COM, NTLDR	(none)
AUTOEXEC.BAT, CONFIG.SYS	Installers: Change Everyone: Read Server Operators: Change
C:\TEMP	Everyone: (RWXD)*(NotSpec)
C:\WINNT\	Installers: Change Everyone: Read

	Server Operators: Change
files	Everyone: Read Server Operators: Change
win.ini	Installers: Change Public: Read Server Operators: Change
Control.ini	Installers: Change Everyone: Read Server Operators: Change
Netlogon.chg	(none)
\WINNT\config\	Installers: Change Everyone: Read Server Operators: Change
\WINNT\cursors\ \WINNT\fonts	Installers: Change Everyone: Add & Read Server Operators: Change Power Users: Change
\WINNT\help\	Installers: Change Everyone: Add & Read Server Operators: Change Power Users: Change
*.GID, *.FTG, *.FTS	Everyone: Change
\WINNT\inf\	Installers: Change Everyone: Read
*.ADM files	Everyone: Read
*.PNF	Installers: Change Everyone: Read Server Operators: Change
\WINNT\media\	Installers: Change Everyone: Read Server Operators: Change Power Users: Change
*.RMI	Everyone: Change
\WINNT\profiles\	Installers: Add&Read Everyone: (RWX)*(NotSpec)
Dir: (*user name)*	User: Full
Dir: All users	Installers: Change

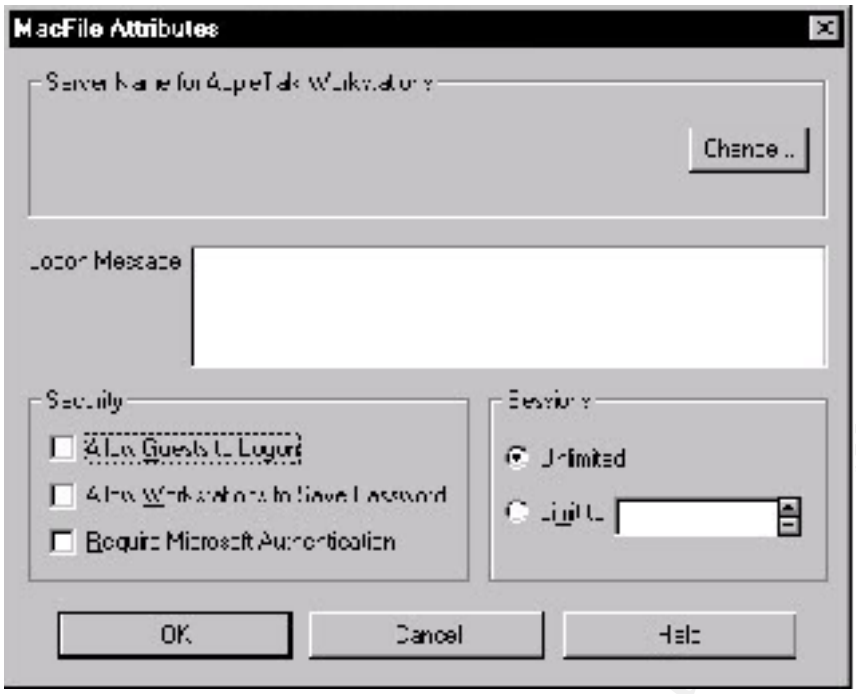
Dir: Default	Everyone: Read
\WINNT\repair\	(none)
\WINNT\system\	Installers: Change Everyone: Read Server Operators: Change
files	Everyone: Read Server Operators: Change
\WINNT\System32\	Installers: Change Everyone: Read Server Operators: Change Backup Operators: Change
files	Everyone: Read Server Operators: Change
$winnt$.inf	Installers: Change Everyone: Read Server Operators: Change
AUTOEXEC.NT, CONFIG.NT	Installers: Change Everyone: Read Server Operators: Change
cmos.ram, midimap.cfg	Everyone: Change
localmon.dll, decpsmon.*, hpmon.*	Installers: Change Everyone: Read Server Operators: Change Print Operators: Change Power Users: Change
\WINNT\System32\config\	Everyone: List
files	(none)
\WINNT\System32\DHCP\	Everyone: Read Server Operators: Change
\WINNT\System32\drivers\ (including \etc subdirectory)	Everyone: Read
\WINNT\System32\LLS	Installers: Change Everyone: Read Server Operators: Change
\WINNT\System32\RAS	Everyone: Read Server Operators: Change

\WINNT\System32\Repl	Everyone: Read Server Operators: Change
\WINNT\System32\Repl\, import, export, and scripts subdirectories	Everyone: Read Server Operators: Change Replicator: Change
\WINNT\System32\spool	Installers: Change Everyone: Read Server Operators: Full Print Operators: Change Power Users: Change
\drivers\ \drivers\w32x86\2\ \prtprocs\ \prtprocs\w32x86\ \drivers\w32x86\	Installers: Change Everyone: Read Server Operators: Full Print Operators: Change Power Users: Change
\printers\, \tmp\	Installers: Change Everyone: (RWX)(NotSpec) Server Operators: Full Print Operators: Change Power Users: (RWXD)(WXD)
\WINNT\System32\viewers	Everyone: Read Server Operators: Change
\WINNT\System32\wins	Everyone: Read Server Operators: Change
C:\...*.EXE,	Everyone: X
C:\…*.BAT, *.COM, *.CMD, *.DLL	Everyone: Read
\WINNT\system32\four BSD r* commands	none

The registry must also be secured for network access. To restrict network access to the registry only to administrators change the permissions on *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\winreg* so that the Local Administrators group has Full Control and no others have access.



If the server is running File Services for Macintosh extra steps must be made to secure access to the server. Go into the Macfile control panel then into the Attributes Dialog. Disable guest access to the Macintosh volumes and disable the ability for users to save their passwords on their workstations.



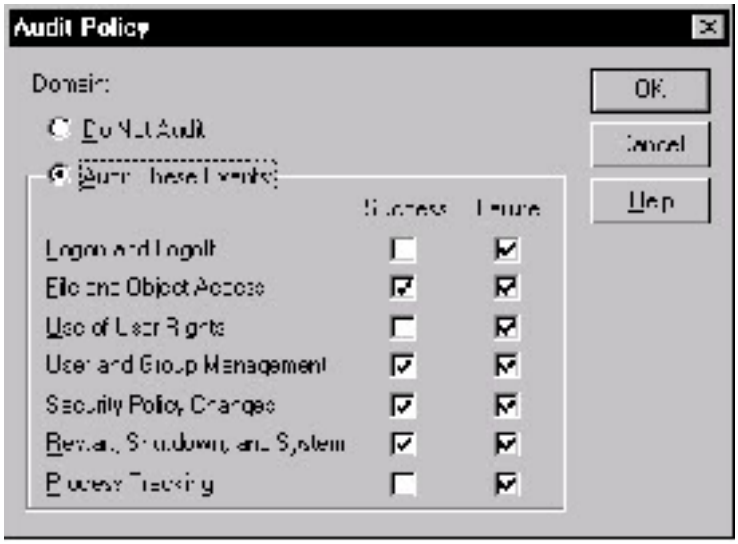
Virus Protection

The final step in protecting your server is to install anti-virus software such as TrendMicro's ServerProtect or Network Associate's NetShield. An anti-virus utility will not only protect your files but can also detect and remove trojan horses that may create new security holes. Make sure to configure your software to scan for all files, not just files with specific extensions. While it will increase the load on your server's resources it is important because new viruses and trojan horses are continually released in forms that may have never been seen before. In addition, non-Windows clients may copy infected files to the server that have no extension at all in the file name.

Your anti-virus software must also be kept up to date. The software should be set to check for updated virus definitions on a daily basis. In addition, it is important to run full scans of the entire server at least once a week. It is possible for the server to become infected with a virus before the vendor is able to release an update to detect that virus. A manual scan will catch the virus even if it was able to slip pass the real-time scan.

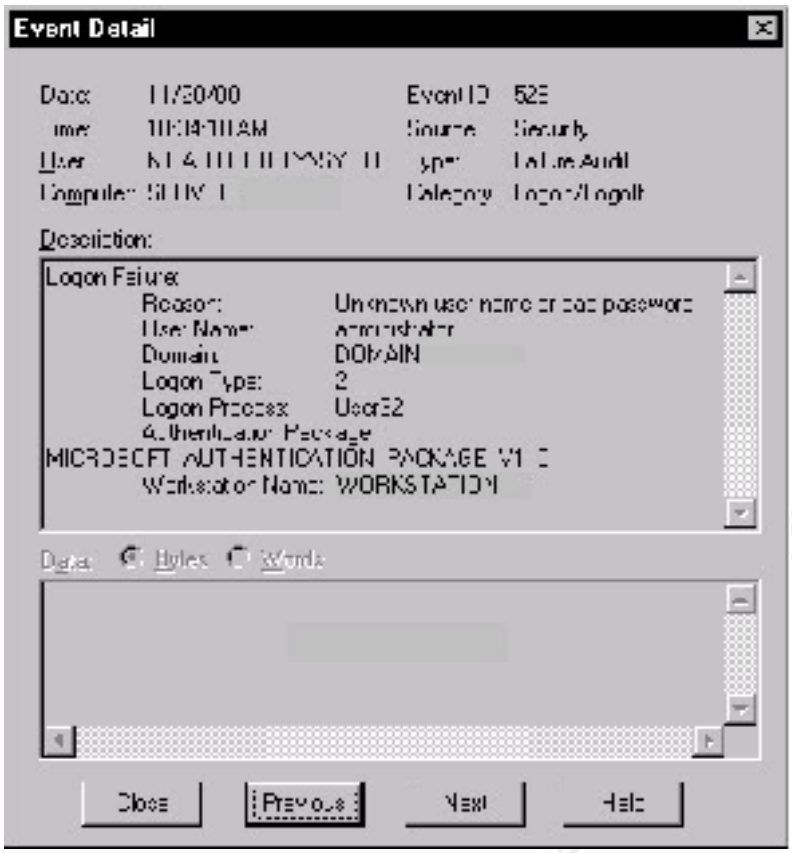
Auditing

Once the server has been secured, it is crucial to maintain consistent and thorough auditing. A strong auditing configuration will alert the administrator to attacks on the server and can reveal additional vulnerabilities. To enable auditing, select Audit Policies in User Manager and choose all the events you wish to monitor.

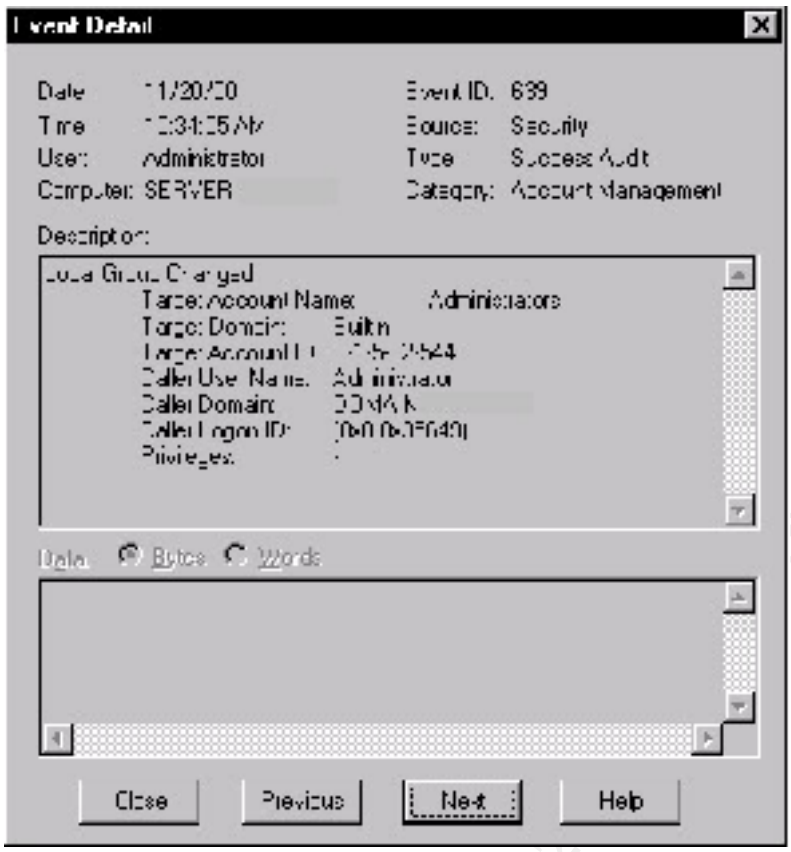


Once auditing is enabled, events can be viewed in the Event Viewer under the Security Log. First the Security Log must be configured properly. In the Event Log Settings dialog, the Maximum Log Size should be set as large as possible without taking up too much space on the server. Next, the Event Log Wrapping should be set to either overwrite after at least 7 days (or however long is necessary to ensure a full backup of the log) or set to Clear Log Manually. It should not be set to Overwrite Events as Needed since if the log fills too quickly, older events that may contain important information could be overwritten.

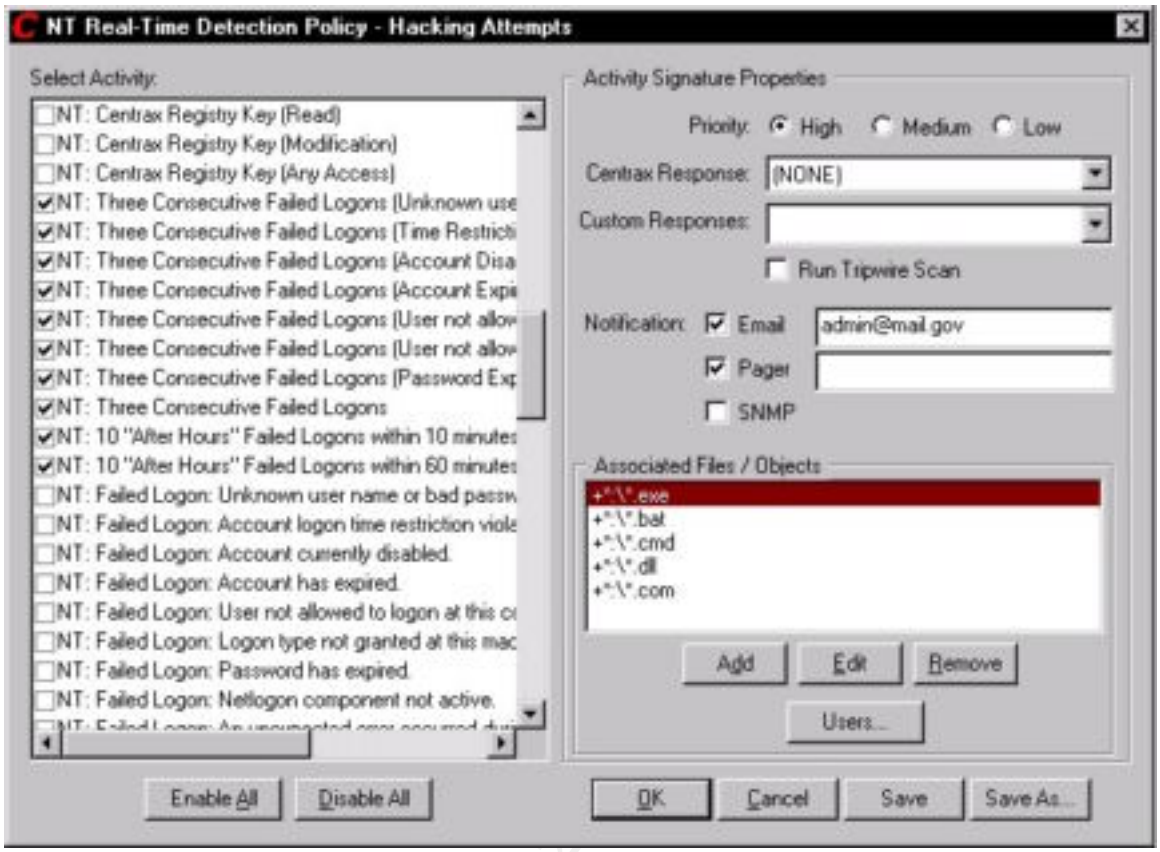
The logs should be routinely monitored. Extra attention should be paid to events such as numerous failed logon attempts, a failed logon attempt with the Administrator account,



or changes to the Administrators group.



Continually monitoring the event logs would be difficult even on a small network and impossible on any large-scale network. An Intrusion Detection System can be set to automatically monitor and analyze the event logs and send alerts when the network is being attacked. With a utility such as CyberSafe's Centrax, the administrator can create detailed conditions on when to be alerted of unusual events in the Security Log and be notified via e-mail or a pager.



References

Albright, John W., "Limiting Anonymous Logon/Network Access To Named Pipes and Shares", 2000. http://www.sans.org/y2k/practical/John_Albright.doc

Fossen, Jason and Jennifer Kolde, Securing Windows NT, Step-by-Step, The SANS Institute, 2000.

Gabert, Howard F., "Using Event Logs to Audit Windows NT4", 2000. http://www.sans.org/y2k/practical/Howard_Gabert.doc

Microsoft, "HOWTO: Password Change Filtering & Notification in Windows NT", Microsoft Knowledge Base Article ID: Q151082. http://support.microsoft.com/support/kb/articles/Q151/0/82.asp

Microsoft "Windows NT 4.0 Domain Controller Configuration Checklist" http://www.microsoft.com/technet/security/dccklst.asp

Microsoft, "Windows NT System Key Permits Strong Encryption of the SAM", Microsoft Knowledge Base Article ID: Q143475. http://support.microsoft.com/support/kb/articles/Q143/4/75.asp

Sutton, Steve, "Windows NT Security Guidelines", Trusted Systems Services, 1999. http://www.trustedsystems.com/download/NSAGuideV2.PDF

Last Updated: July 22nd, 2017

Upcoming Training

SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**