Global Information Assurance Certification Paper

GIAC SECURING WINDOWS NT

PRACTICAL ASSIGNMENT

Laura Kraus

Table of Contents

Introduction

The securing of a Windows NT server is an ongoing process where vulnerability and functionality must be balanced. There are many procedures that can be performed in order to fully secure a Windows NT server. I am only going to provide you with a description and demonstration of a few of the most basic tasks that must be performed to start the securing of a Windows NT server.

Section 1 Physical Security

A Windows NT server is at risk of being stolen or physically destroyed. Actions must be taken to prevent such disaster from occurring.

Physical Access

Physical access to the server must be restricted. The proper location is essential to providing physical security to a Windows NT server. Placing the server in a locked room and monitoring access through the use of video cameras, card keys and other entry auditing devices will lower server vulnerability to theft.

Physical Destruction

The placement of uninterrupted power supplies will protect against power surges and outages. UPS's that interact with the server to shut down the server gracefully in the event of a power failure will prevent damage to servers. American Power Conversion (APC) manufactures Smart-UPS's and power management software called PowerChute Plus that facilitates unattended operation of servers, power quality data logging, shutdown notification and control, auto-restarting, diagnostics, and battery conservation features.

The regulation of temperature and humidity are other environmental variables that should be monitored and regulated to provide an optimal environment for server function. HVAC systems can be installed to monitor all environmental variables and can be configured to send alerts via e-mail or pages.

Section 2 Hardware Security

Prevent Rebooting

Actions should be taken to prevent attackers from restarting the server and booting off a floppy disk with an operating system and utilities that allow the bypassing of Windows NT security. The BIOS can be configured to disable the ability to boot from any device other than the hard drive. A BIOS password must be set on the server to prevent changing of the boot order to the floppy disk drive. Another option to consider is the

removal of the system's floppy and CD-ROM drives to prevent booting from them. The only downfall to this method is that there is a negative impact and increased delay to disaster recovery efforts.

Secure Media
Securing media such as tape backup cartridges and emergency repair disks that contain the SAM and other highly sensitive data can prevent its theft or destruction. This can be accomplished by locking media in a fireproof safe or by archiving copies to an offsite storage facility.

Section 3 File/Software Security

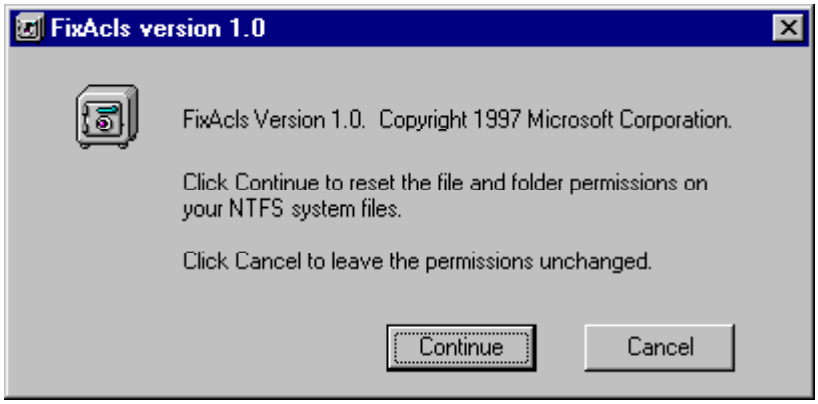
File System
Windows NT supports both File Allocation Table (FAT) and New Technology File System (NTFS) file systems. NTFS should be used on all volumes to maximize security. NTFS supports over the network and local console file and folder access permissions. NTFS also supports detailed auditing of file and folder access.

A non-destructive method for converting a FAT volume to NTFS can be accomplished by running the convert utility.

1. Open a command prompt and type *convert [drive letter]: /fs:ntfs* then press enter.

If the volume to be converted contains the current boot partition the conversion will not take place until the next reboot.

Once the volume has been converted the NTFS file permissions will be set to Everyone:Full Control. To set the permissions back to Windows NT default, a utility called fixacls.exe should be run. This utility can be obtained from the Windows NT 4 Resource Kit.



Service Packs

Service packs are how Windows NT product updates are distributed. Service packs keep the product current, extending and updating your computer's functionality. Service packs include updates, system administration tools, drivers, and additional components. All are conveniently bundled for easy downloading. Service packs are cumulative -- each new service pack contains all the fixes in previous service packs, as well as any new fixes. You do not need to install a previous service pack before you install the latest one. (Source: Microsoft Knowledge Base Article ID: Q152735)

To check if the latest service pack has been installed on a server:

1. Click Start then click Run…
2. Type "*winver*".

If the About Window NT Box contains “Revised Service Pack 6a” then the server is running the latest version of service pack. If that line is not present the latest service pack can be downloaded at:

http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/allSP6.asp

Hot Fixes
In addition to installing the latest service pack, it is important to obtain the latest hot fixes or security patches that are released between service packs. Their releases are generally in response to a new found vulnerability in Window NT. The latest hot fixes can be downloaded at:

http://www.microsoft.com/ntserver/nts/downloads/

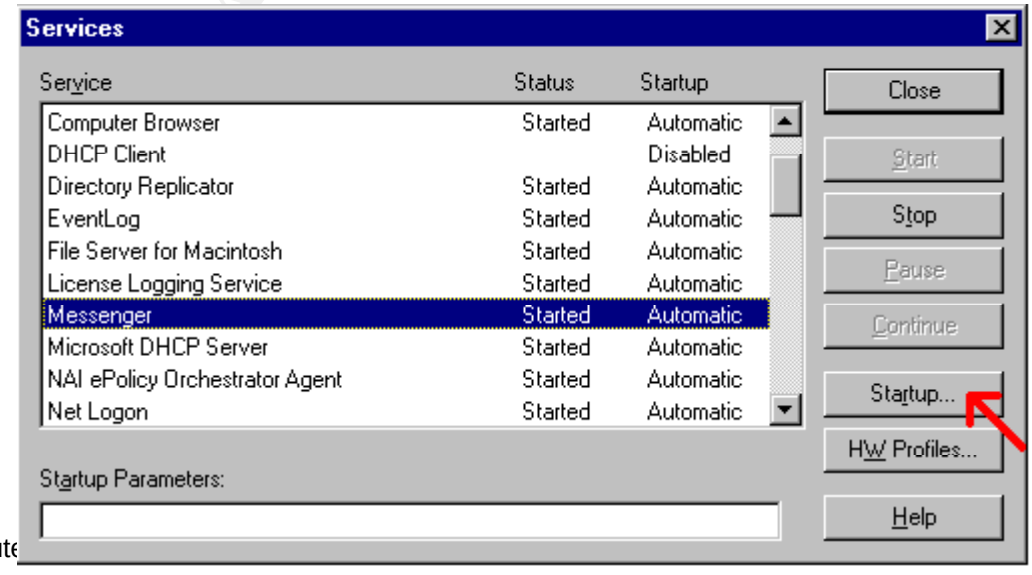
Virus Software
Viruses are a constant threat to Windows NT. The number of viruses and malicious viral attacks has grown at an enormous rate. Installing virus protection, configuring scheduled scans and constantly updating definition files can help prevent the destruction of servers due to viral infection.

Section 4 Stripping Down the System

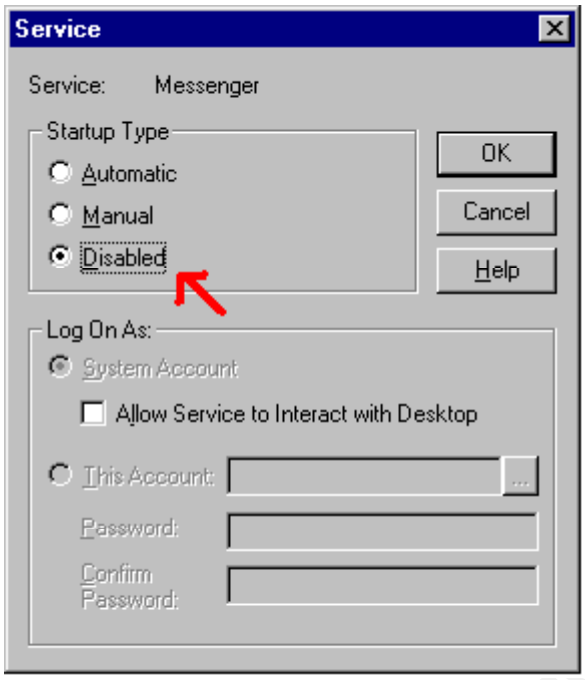
Disabling unnecessary services, features, protocols and bindings will decrease your vulnerability by creating less potential methods of attack.

Services
Non-essential services that are running by default can be disable to eliminate the risk of their use to compromise the system.

To disable unnecessary services:
1. Click Start, Control Panel then Services;
2. Select the service to be disable then Click Startup…



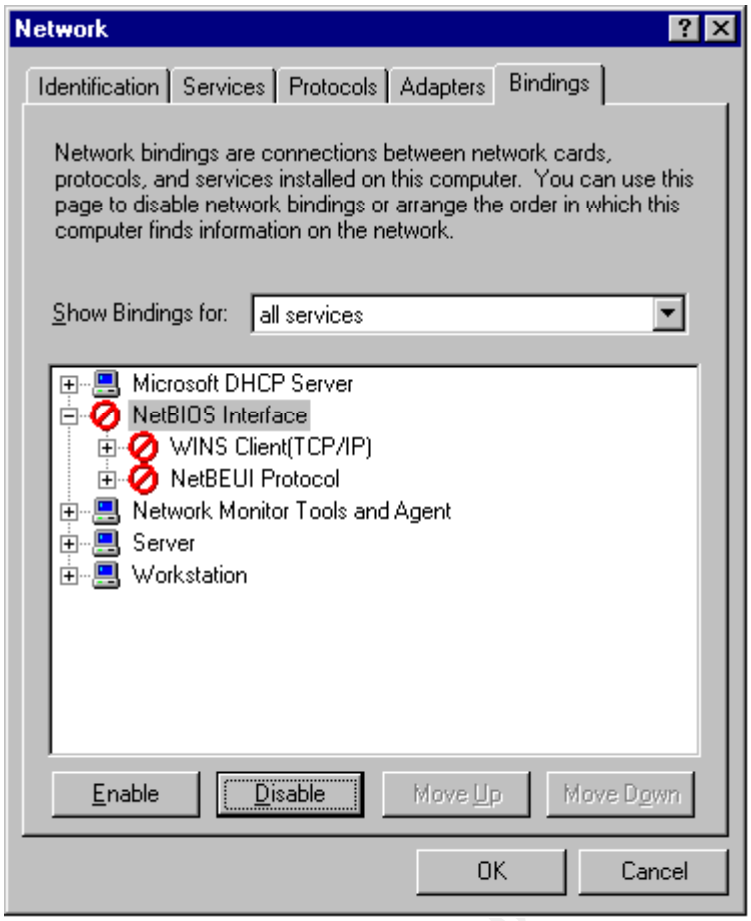
3. Choose disable then click OK.



At this point clicking the stop button can stop the service. Disabled services will not start when the server is rebooted and will no longer be a cause of vulnerability.

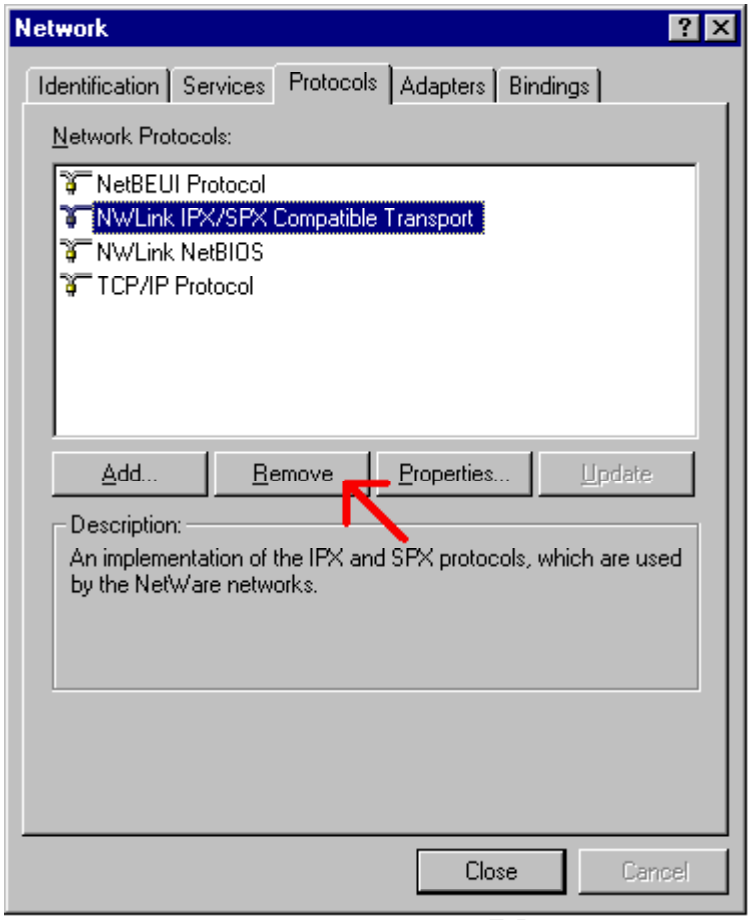
Protocols
Unbind unnecessary protocols like IPX/SPX or NetBIOS from the network adapter to prevent denial-of service attacks against that protocol.

To unbind unused network services:
1. Click Start, Control Panels then Network;
2. Select the Bindings tab and then “all services” from the pull-down menu.
3. Double-click the service then click Disable.



To unbind unused protocols:

1. Click Start, Control Panels then Network;
2. Select the Protocols tab and unused protocol then click Remove.



OS/2 and POSIX

The OS/2 and POSIX Subsystems are not necessary for most applications and services and should be removed to prevent their use attacks against Windows NT.

To remove OS/2 and POSIX subsystems do the following.

1. Delete the *\winnt\system32\os2* directory and any subdirectories.
2. Then edit the registry using the following chart.

Hive	HKEY_LOCAL_MACHINE\SOFTWARE
Key	\Microsoft\OS/2 Subsystem for NT
Action	Delete all sub keys
Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	\CurrentControlSet\Control\Session Manager\Environment
Value Name	Os2LibPath
Action	Delete
Hive Key	\CurrentControlSet\Control\Session Manager\SubSystems
Value Name	Optional

Action	Delete values
Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	\CurrentControlSet\Control\Session Manager\SubSystems
Action	Delete entries for Posix and OS/2

The settings will take effect when the system is rebooted.

The stripping down of the system by removing unnecessary services, features, protocols and bindings will eliminate them as potential means of attack.

Section 5 Account Security

Built-in Accounts

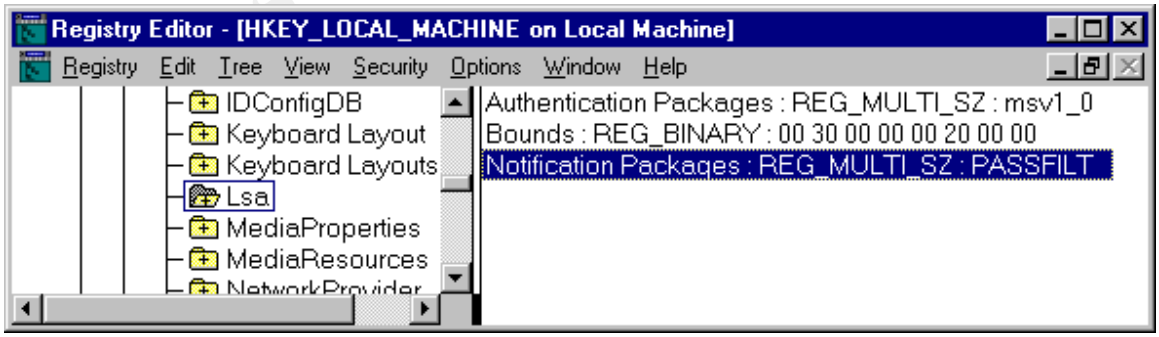
The Administrator account should be renamed and given a strong password. Account lockout should be enabled for the Administrator account by using the utility PASSPROP.EXE. The Guest account should be giving a non-blank password and disabled.

Password Filter

A password filter (PASSFILT.DLL) can be added to ensure new passwords be at least six characters, not contain any part of the user's name and must contain at least three of the following four types of characters: uppercase letters, lowercase letters, numbers or non-alphanumeric symbols. A filter can be applied by making the following registry change:

Hive	HKEY_LOCAL_MACHINE
Key	\System\CurrentControlSet\Control\Lsa
Value Name	Notification Packages
Value Type	REG_MULTI_SZ
Value Data	PASSFILT

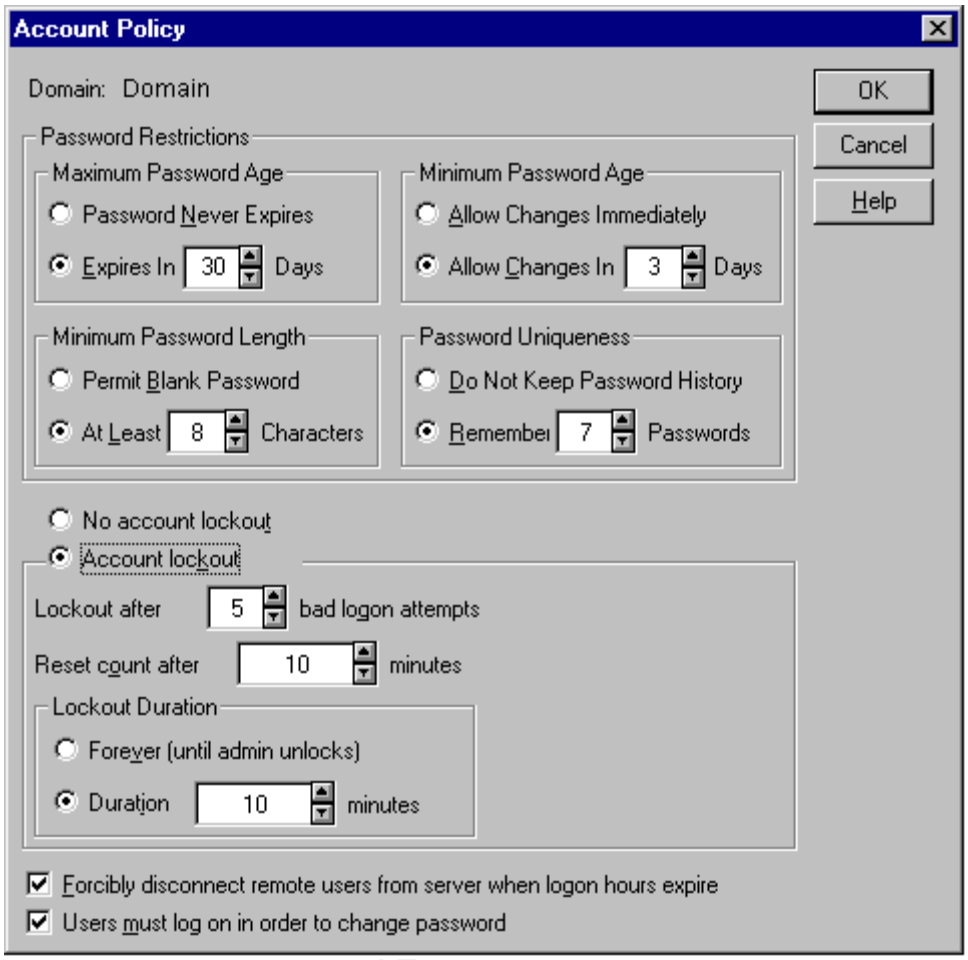
Registry with PASSFILT.DLL in use



Password Policies

Password policies should be configured for all users in a domain. This can be completed the following:

1. Open User Manager, click on Policies then Account…
2. The policy may vary depending on the level of password security necessary.



SYSKEY.EXE

SYSKEY.EXE is a utility that can be used to encrypt the Security Accounts Manager (SAM). SYSKEY.EXE offers strong encryption that protects account information by encrypting the password data using a 128-bit random key. The System Key is then used to encrypt the 128-bit random key. When running SYSKEY.EXE the network administrator is given the three options for storing the System Key. Choosing the placement of the System Key depends on the environment where the security is implemented.

More information on SYSKEY.EXE is available from (Microsoft Knowledge Base Article ID: Q143475).

Encrypting the passwords in the SAM is important in preventing the breaking of password with utilities like L0phtCrack by L0pht Heavy Industries http://www.l0pht.com.

NTLMv2 Authentication
NTLMv1 authentication can make it possible to crack passwords with utilities during the challenge/response authentication session between Windows NT servers and clients. This makes it imperative that NTLMv2 be used instead of NTLMv1. To enable NTLMv2 on Windows NT make the following registry changes.

Hive	HKEY_LOCAL_MACHINE
Key	\System\CurrentControlSet\Control\Lsa
Value Name	LMCompatibilityLevel
Value Type	REG_DWORD
Value Data	0 to 5

The value data can be set to a single digit between 0 and 5. The level of security will depend on which value is used.

Section 6 File Sharing Security

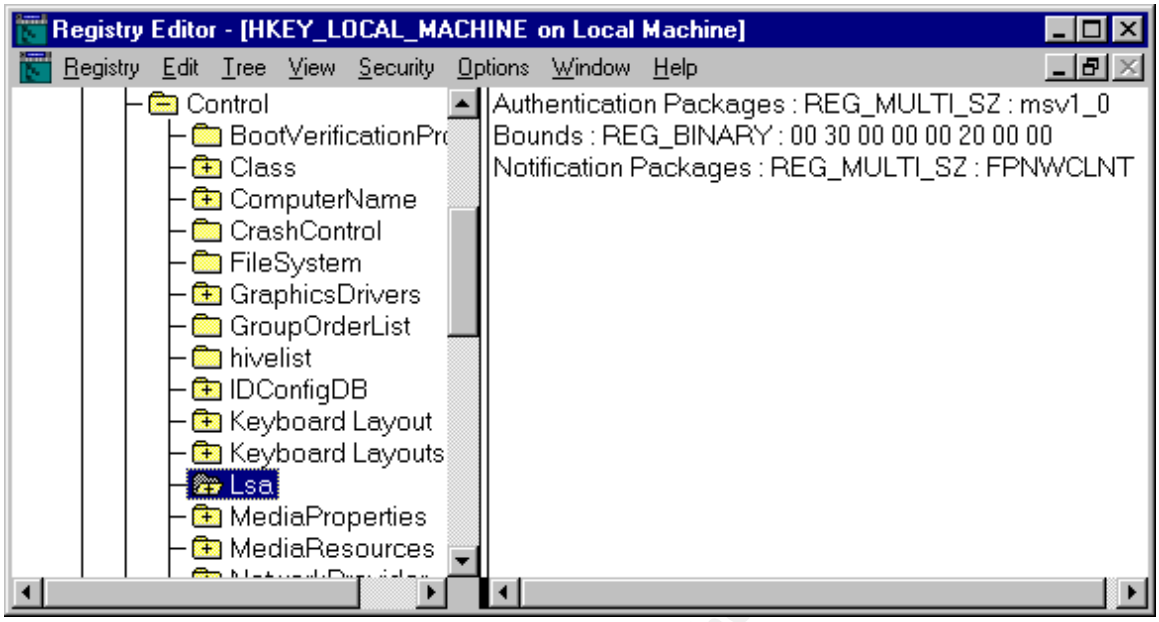
To minimize exposure to attack it is essential to limit and restrict access to shared files and folders on a Windows NT server. Often functionality must be forgone in the sake of securing a system. Some or all of the following procedures may or may not be appropriate for all machines.

Null sessions
Null sessions are mainly used for administrative purposes and communication between network services. Null sessions are built into the operating system and are considered a major security hole but are often necessary for server functionality. Making changes in the registry can restrict null sessions.

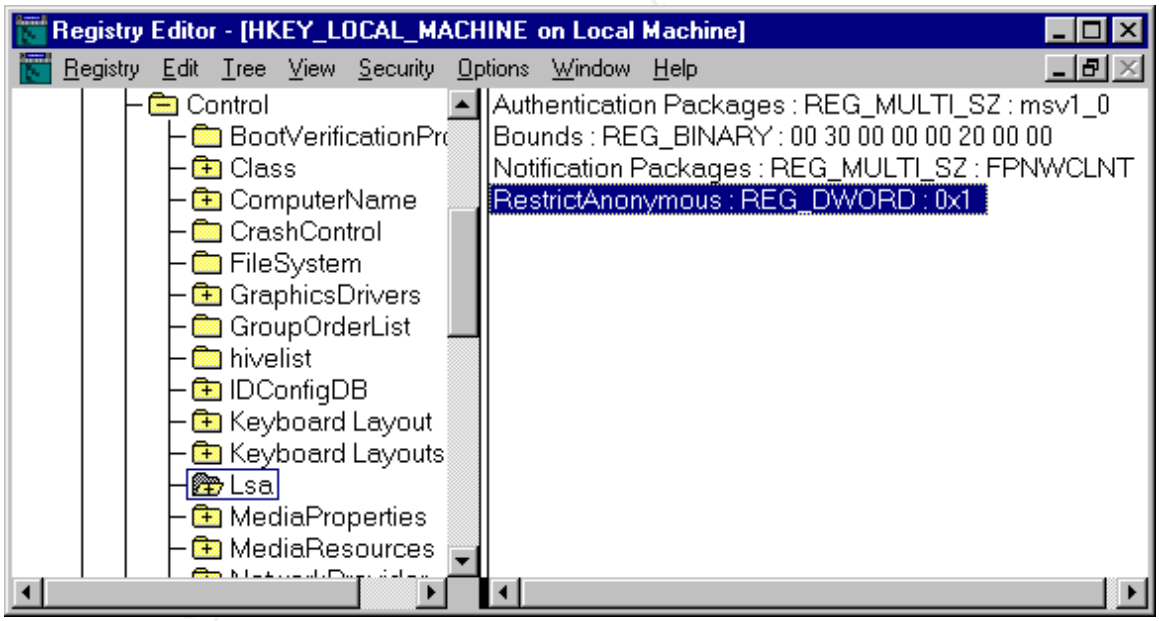
To prevent null sessions users from viewing share names, remotely add the following registry settings.

Hive	HKEY_LOCAL_MACHINE
Key	\System\CurrentControlSet\Control\LSA
Value Name	RestrictAnonymous
Value Type	REG_DWORD
Value Data	1

Registry before changes



Registry after changes

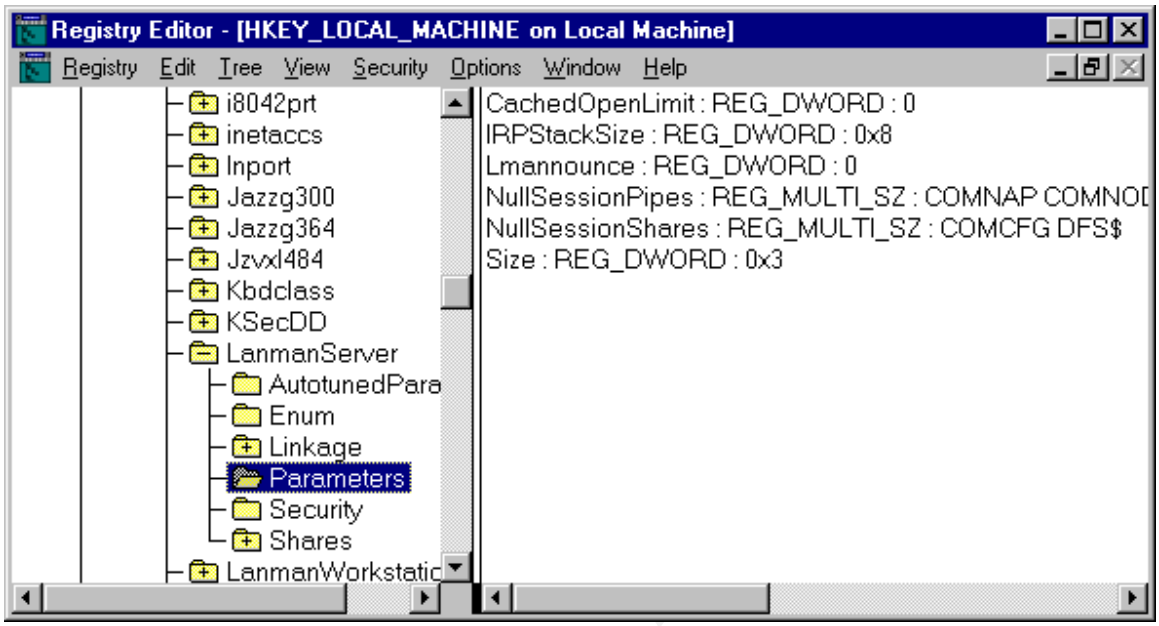


The default setting for null session access to shares is on. With this setting null session users are assigned the same share permission access as the Everyone group. To restrict access to null session shares make the following changes to the registry:

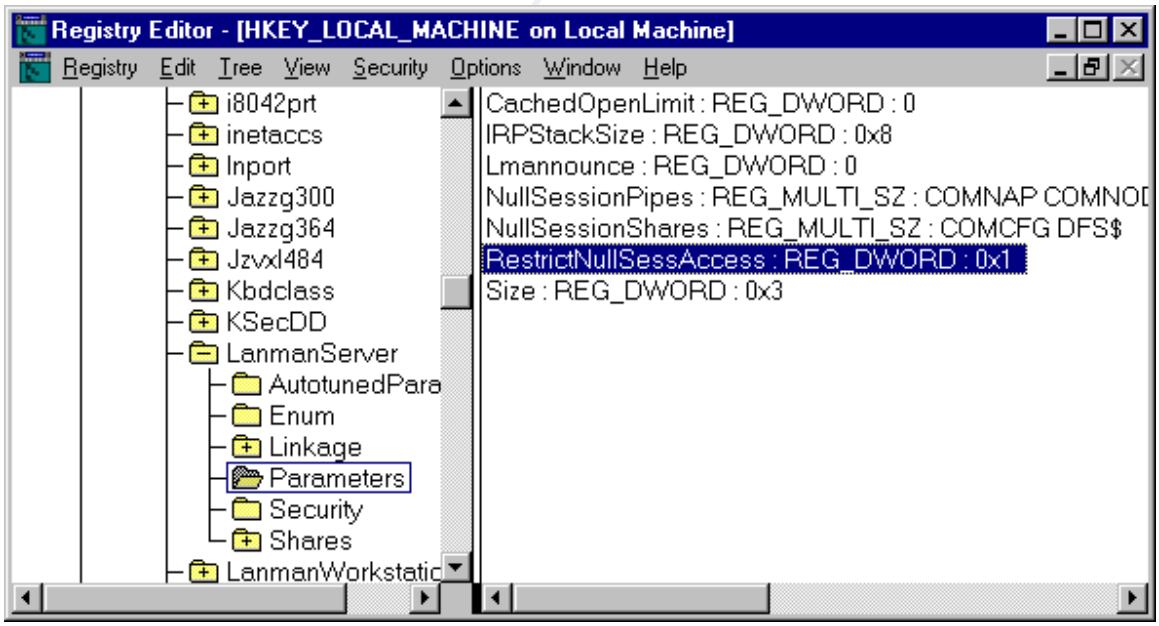
Hive	HKEY_LOCAL_MACHINE
Key	\System\CurrentControlSet\Services\LanmanServer\Parameters
Value Name	RestrictNullSessAccess
Value Type	REG_DWORD

Value Data	1

Registry before changes



Registry after changes



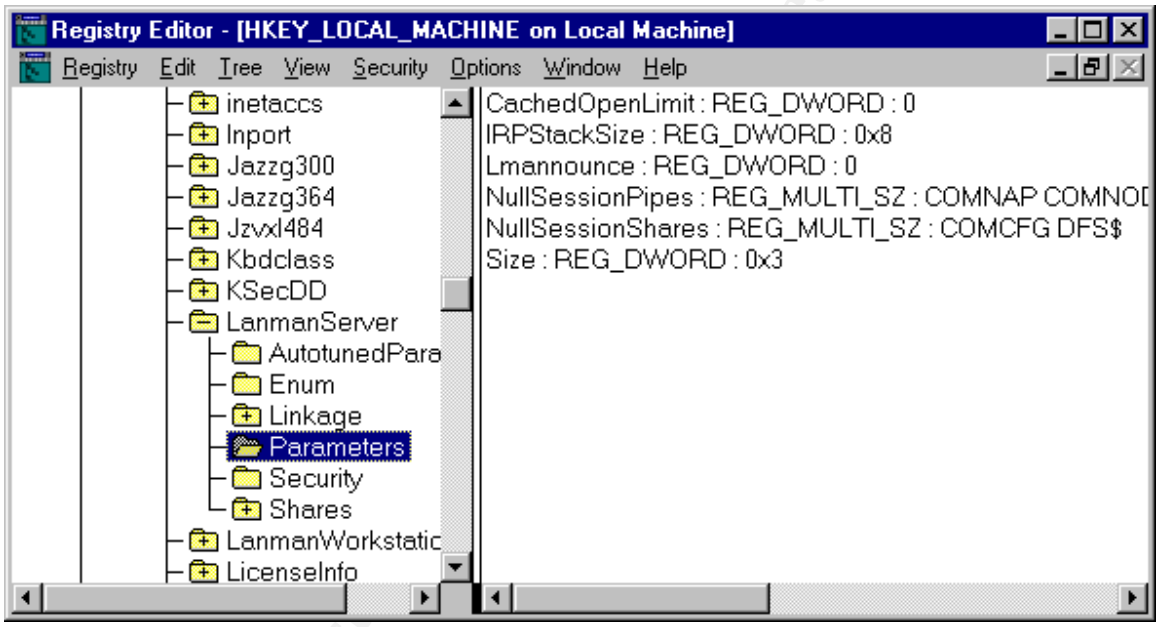
One thing to take under consideration is that the built-in system account and certain applications may need to use null sessions to access shares.

Disable Administrative Shares

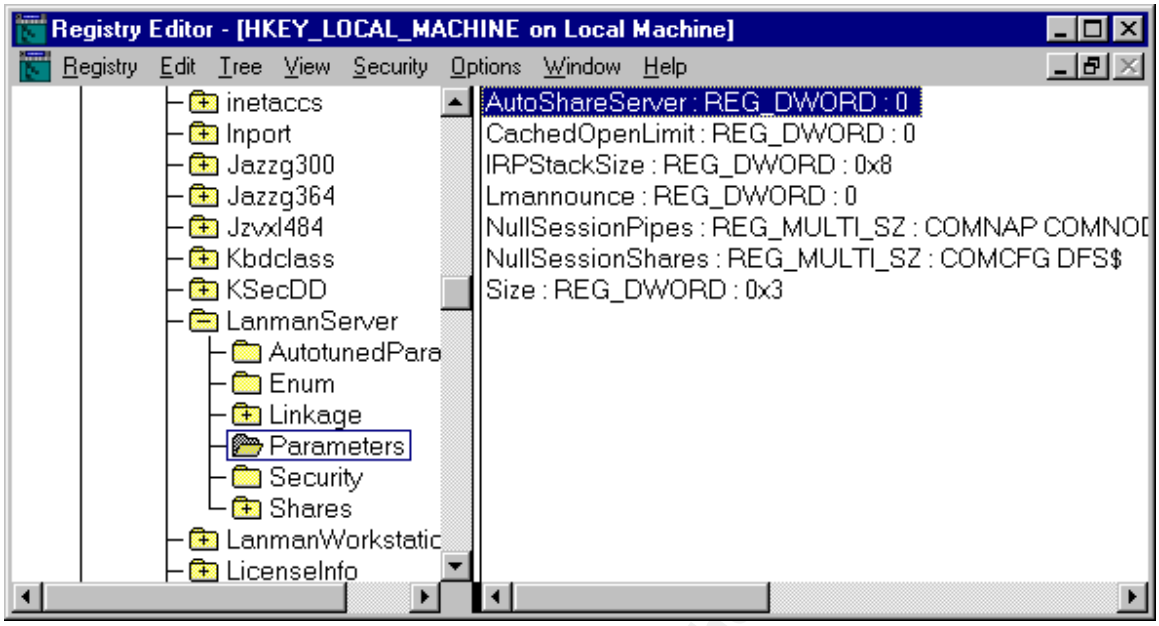
Administrative shares are automatically present on all Windows NT computers. The shares are hidden and named after their perspective volume i.e., C$, D$, E$, etc. The %SystemRoot% folder that typically is C:\Winnt is shared as Read only under the share name ADMIN$. It is good practice to disable this feature when ever possible. To disable administrative shares add the following to the registry:

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

Registry before changes



Registry after changes



It is important to keep in mind when disabling administrative shares that their absence make it more difficult to remotely administer, and some network applications rely on those shares.

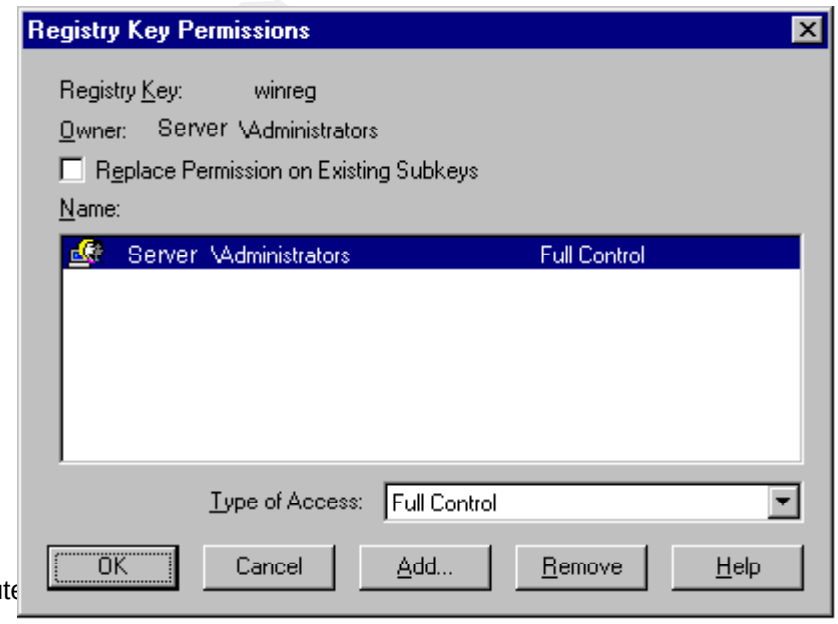
Network Access to the Registry

Network access to the registry is controlled by the permissions set on the Winreg registry key. To restrict remote access to the registry, complete the following steps:

1. Locate the following key in the registry:

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	\System\CurrentControlSet\Control\SecurePipeServers\Winreg

2. Select the Winreg key, click Security, then Permissions.
3. Set the Administrators permission to Full Control but make sure that no other user or



group is listed. Then click ok.
More information on regulating network access to the registry can be obtained from the Microsoft Knowledge Base Article ID: Q155363.

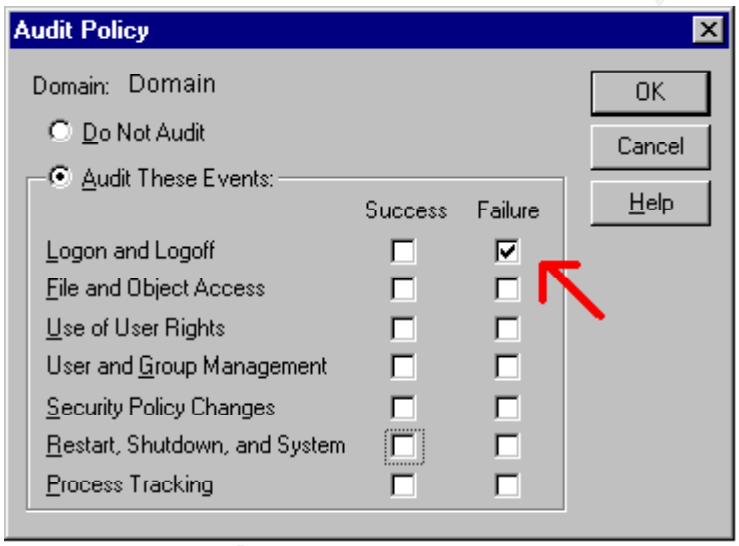
Section 7 Auditing

Auditing is a security feature built into Windows NT that allows the selection of categories of events to be logged to a file. Events selected for auditing are stored in the system and security logs, which can be viewed with the Event Viewer Utility.

Auditing Logon Failures

Auditing is crucial for monitoring events that reflect attempts made by an intruder to logon. To enable auditing of logon failures complete the following steps:

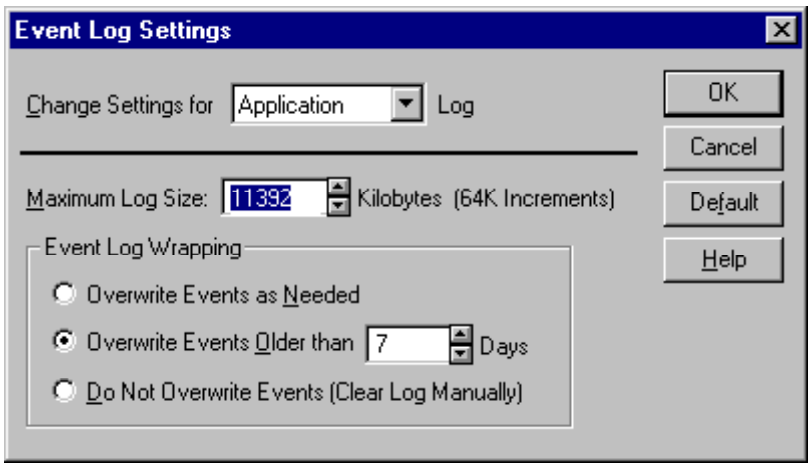
1. Open User Manager, Click Policies then Audit;
2. Check the box under Failure that corresponds with Logon and Logoff.
3. Then click ok.



Event Viewer

The Event Viewer can be used to view the logs of audited events. It is important to configure the log size and wrapping option in order to prevent the loss of critical logged events. To change the settings do the following:

1. Open Event Viewer, click on Log, then Log Settings…
2. Make the changes, then click OK.



It is important to configure the Event Log Setting in accordance to the variables and environment in which it is used.

Security Configuration Manager
Security Configuration Manager (SCM) is an integrated security system that gives administrators the ability to define and apply security configurations for Windows NT Workstation and Windows NT Server installations. SCM also has the capability to perform inspections of the installed systems by locating any degradation in the system's security. (Source: Microsoft Knowledge Base Article ID: Q195227)

Security Configuration Manager can be downloaded at:
http://support.microsoft.com/support/kb/articles/q195/2/27.asp

Instructions on using Security Configuration Manager is available at:
http://www.microsoft.com/ntserver/security/techdetails/prodarch/securconfig.asp

Section 8 Keeping up

Securing Windows NT server is an ongoing battle. In order stay on top of the latest security procedures, it is important to monitor security related web sites and bulletin boards for newly discovered vulnerabilities.

Microsoft has a web site that is regularly updated with the latest patches and fixes. That can be found at:
http://microsoft.com/technet/security/default.asp

References

Fossen, Jason, J. Kolde, "*Securing Windows NT, Step-by-Step, Parts 1-3*" Ver 3.7
SANS conference notes Monterey, CA October 15-22, 2000

Schultz, E. Eugene, "*Windows NT/2000 Network Security"* , MTP, 2000

Strebe, Matthew "*NT Server 4, 24 seven",* SYBEX Inc., 1999

Moncur, Michael "*MCSE The Core Exams in a Nutshell"*, O'Reilly & Associates, Inc., 1998

Saddique, Mohammed "*SERVER SECURITY FOR A DOMINO SERVER",* GIAC Securing Windows NT

Gabert, Howard "*Using Event Logs to Audit Windows NT4",* Practical Assignment for SANS GIAC Training, Securing Windows NT, Ottawa, Ontario Canada, August, 2000

How to Obtain the Latest Windows NT 4.0 Service Pack - Microsoft Knowledge Base Article ID: Q152734

How to Regulate Network Access to the Windows NT Registry- Microsoft Knowledge Base Article ID: Q155363

Windows NT System Key Permits Strong Encryption of the SAM- Microsoft Knowledge Base Article ID: Q143475

Windows NT 4.0 Domain Controller Configuration Checklist
http://www.microsoft.com/technet/security/dccklst.asp?a=printable#seclm