Global Information Assurance Certification Paper

Auditing Windows NT
Sheng Huang

Introduction

Windows NT comes in two flavors, Windows NT Workstation and Windows NT Server. Windows NT Workstation is designed to be a powerful desktop operation system, and the Windows NT Server is designed to provide resources sharing in a heterogeneous network environment. Windows NT only provides minimum-security protections by default. To really secure Windows NT systems, it requires numerous steps and careful planning depending on the deploying environment. The goal of this paper is to explain and provide crucial step-by-step procedures on how to secure and audit Windows NT systems.

The paper includes procedures on adding and changing the Windows NT registry key settings. It is recommended to export the current registry setting by using registry tool, regedit.exe and save it in a removable media for system recovery. All registry modification should be tested on a non-production environment first.

Audit Planning

Audit planning requires a fair amount of preparation. Before auditing any systems, collect and review your company's security policies on Windows networks. The policies should include user password complexity requirement, system executables permissions settings, SAM databases maintenance, system usage policy and etc. Then decide what to audit, how to collect the information, and how to delivery your findings. Any auditing should be started with an Entrance Conference. The purpose of this meeting is to inform the IS personnel how you are going to conduct your audit, and what they can expect, and identifying the other system administrators' concerns.

Service Pack and Hot Fix

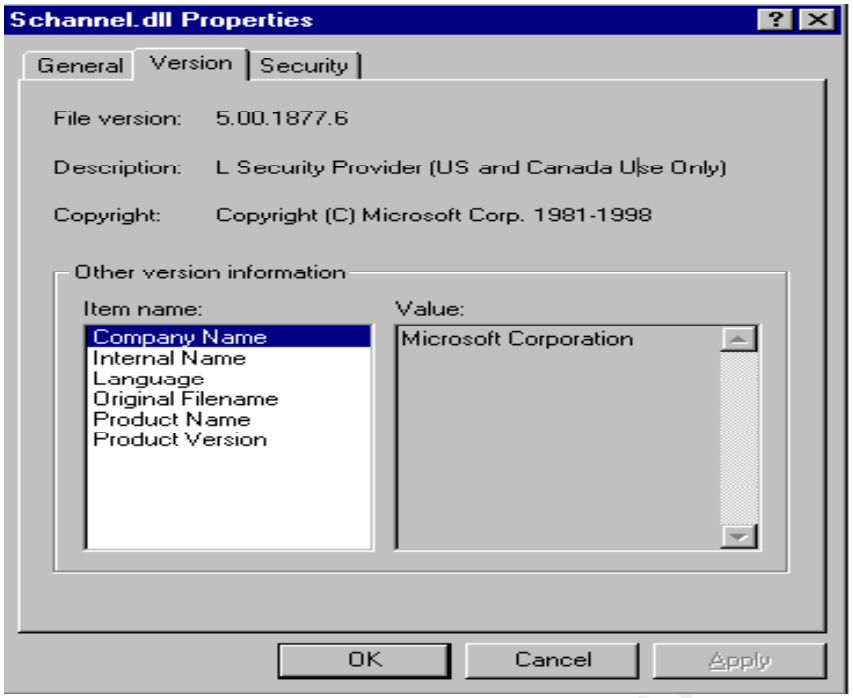
Service Pack is a collection of updates and patches for Windows NT. The latest Service Pack can be downloaded for free from Microsoft "http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/allSP6.asp". The Windows NT service pack has two versions. One is for the North American region; another is for the rest of the world. The domestic version, for North American region, provides 128-bit encryption services. The export version, for the rest of the world, provides 40-bit encryption services. It is highly recommended to install the high Encryption version for North American users.

Microsoft continuously release new patches and Hotfixes to make Windows NT become a more robust and secured operating system. These new patches and Hotfixes usually bundled together and named "Hotfixes-post<last release version of service pack>" before they become a part of new Service Pack release. Since these patches and Hotfixes are not thoroughly tested, it is recommended as installed-on-the-need base, and should also do your own test on a non-production system before deployed them. Hotfixes can also be downloaded for free from Microsoft's ftp site "ftp://ftp.Microsoft.com/bussys/winnt/winnt-pubic/fixes/usa/nt40". Individual Hotfix could be deployed to the system by double click on the Hotfix icon and select yes on all installation dialogs. It will be handy to have a brief document on all Hotfixes you deployed on production system for later network auditor.

To check encryption level on your Windows NT system

1. Click Start, point to find, then click files or Folder…. Option
2. Type schannel.dll into the Name field, click Search
3. Right click on Schannel.dll, select Properties option, click on the Version tab

If the description indicates "US and Canada Use Only", which means you have 128-bit encryption service installed in your system, otherwise means you only have a 40-bit system.



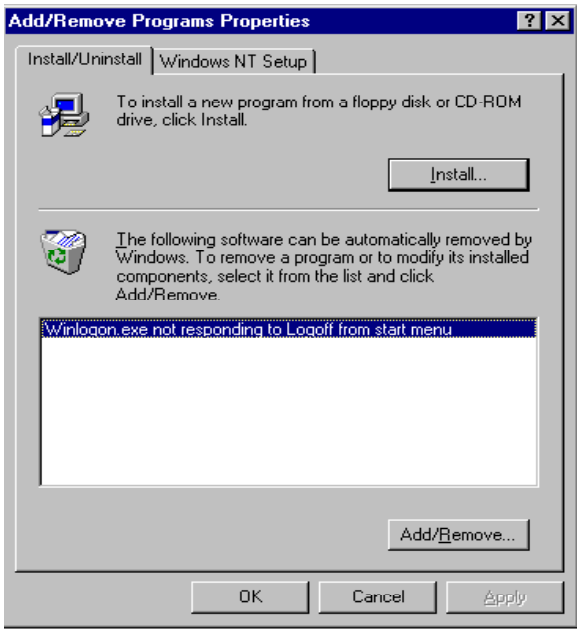
To check what version of Service Pack installed in your system, open the About Window under the Help walk-down menu on any system information window or launch winver.exe from the Start > Run.

The above window indicates the system has Service Pack 6 installed. All Windows NT systems should at lease have Service Pack 4 installed on it.

To check what Hotfixes has been installed in your system

1. Launch the Control Panel
2. Double on the Add/Remove Programs

3. Click at the Install/Uninstall tab
4. Check for long descriptive name on .dll and .exe files



The above window shows that the system installed the Hotfix, which patched the winlogon.exe to fix the logoff operation from the Start menu.

Password and Logon Policies

Username and password are the means by which a user authenticates him/herself to the accessing system against the SAM (security account manager) database. After authenticated, the SAM generates an access token representing the user and the user's group memberships and passes it to the WinLogon process. The WinLogon process then tells Win32 subsystem to create a new process for the user with the security token attached.

When a process attempts to access any object, the process's access token is checked against the ACL (access control list) of the object. The process kept alive until the logon session completed.

Username and password are the keys to launch the access process. It is good practices not to display the last logon user name in a publicly shared system, disable password Caching and restrict the complexity of all users passwords to meet certain network password security standard.

Displaying the last successful login username on the login windows reveals the existing of user account. It reduces the efforts to hack into the system.

To hide the last username in login dialogue

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

By default, Windows NT caches the credentials of the last ten logged on users. Cached credentials are used when a user attempts to log on, but no domain controller is available for authentication. Any user with cached credentials can still log on. This allows a user to log on even if his account has been removed or disabled.

To disable the caching of logon credentials

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

With Windows NT Service Pack 2 or later, a service passfilt.dll is available to enforce complexity of user passwords. Before deploy the following registry setting, ensure your system is patched with Service Pack 2 or higher.

Before configure a system to filter password, a user password complexity policy must be

laid out first. The password complexity policy could be implemented by using the User Manager on a Windows NT Workstation or Domain User Manager on a Windows NT Server.

The password complexity policy include the following attributes:

Maximum Password Age
This attribute controls the expiration period of the password. It's value should be set between 30 to 90 days, depending on the system's security compliant level. **Never** set this attribute to "Password Never Expires" for regular users.

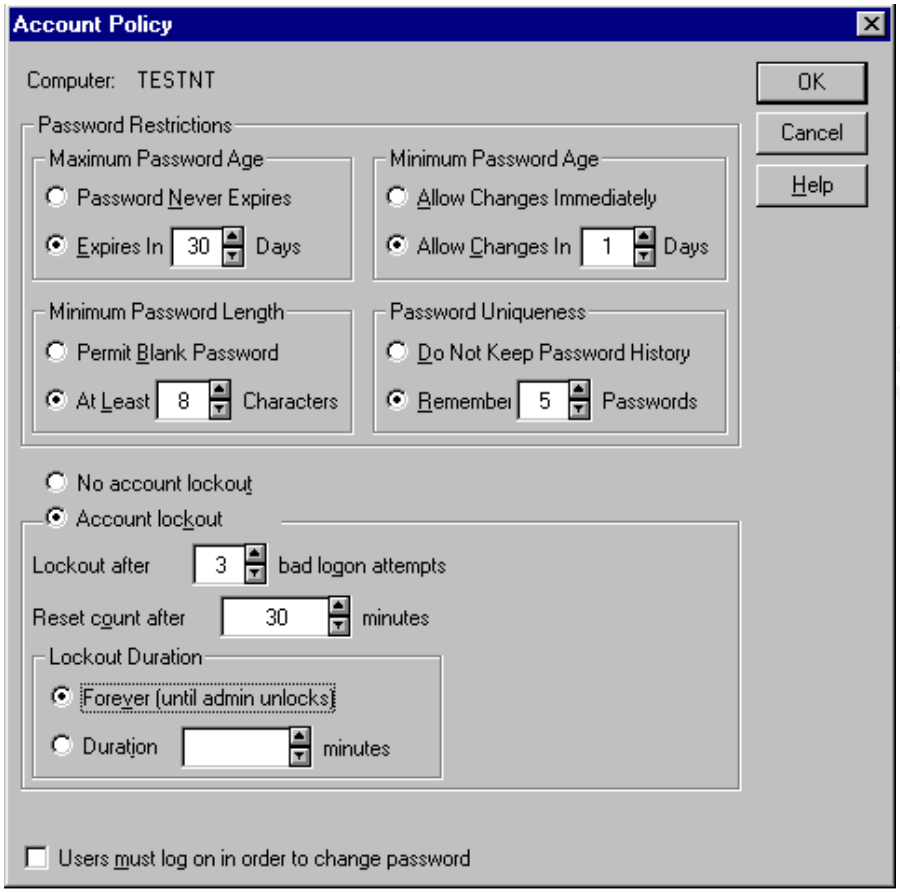
Minimum Password Age
This attribute controls the period between password update attempts. This setting ensures the uniqueness of user password. The value for this attribute should be set between 1 to 5 days.

Minimum Password Length
This attribute restricts the length of use passwords. The value for this should be in the range between 8 and 16.

Password Uniqueness
This attribute controls how many old passwords the system remembers and uses them to check against the new passwords. This setting prevents the user reuse his/her last number of passwords. The number is usually between 5 to 8.

Account lockout
This attribute protects the systems from hacker attacks. This controls how many failed login attempts will cause the user account to be disabled. The value normally sets to 3 or 5.

Lockout Duration
This attribute controls how long the user account will be in the lockout state. When an account is locked out, it can either be locked out forever or for a specific number of minutes. In high-security network, the account is locked out forever until users have to contact an administrator and request that the account to be re-enabled. In a medium-security network, set this value to 240 minutes. This will prevent a hacker from guessing a significant number of passwords in a short period of time, but still permit users to reacquire control of their accounts. Moreover, a 60-minute lockout will limit the severity of DoS attacks with aim at locking out all users.



The above user password policy can also be set by using the Microsoft Security Editor, which is a snap-in of MMC (Microsoft Manager Consol). The MSE also provides other services to ease the system administrators' task on Windows network security setting. This tool will be discussed later in this paper.

To enforce a strong password policy:

1. Confirm that passfilt.dll is located in \%SystemRoot%\system32 directory
2. Ensure the following setting is in the registry:

Hive:	HKEY_LOCAL_MACHINE
Key:	\SOFTWARE\CurrentControlSet\control\LSA
Value Name:	Notification Packages
Value Type:	REG_MULTI_SZ
Value Data:	PASSFILT

All password policy will not be affected until the next time users changing their passwords.

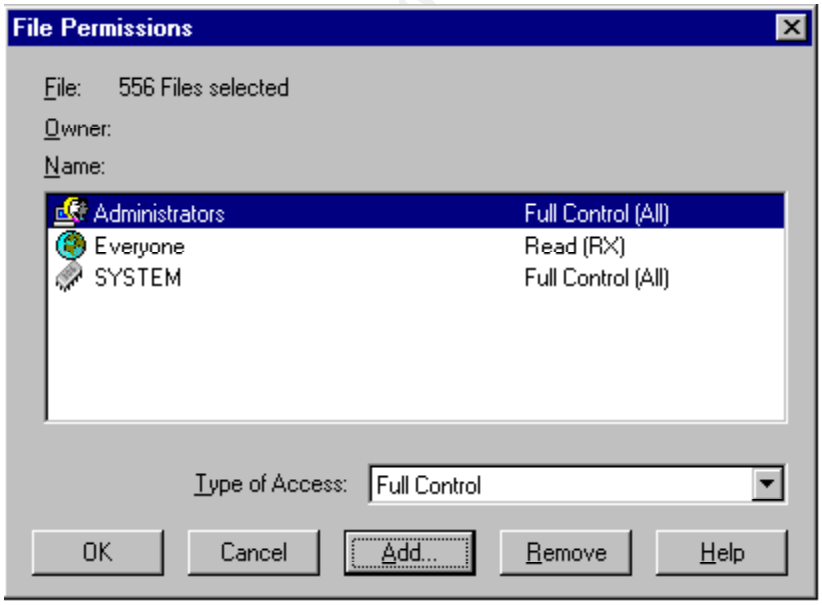
Secure System Executables and System Files

By default, Windows NT installer places all NT files onto drive C. This drive should be NTFS in order to provide audit and access restriction services. Administrators can convert drive from FAT(32) to NTFS by using the command line executable convert.exe with appropriated arguments. The conversion is a one-way process, and there is no way to convert NTFS to FAT. Converting file system to NTFS will prevent access from 9x/Me file system (FAT32 or FAT).

Only the administrator and the system accounts have full control on all batch files, executables and system library files, other user accounts only have read and execute permissions on them. The permission settings prevent system crucial files from modification and the Trojan Horse attacks. File permissions could be set and viewed from the file property operation.

To check the permissions on system files

1. Launch Windows Explorer from Start > Programs
2. Type in *.bat *.exe *.dll onto the named filed and ensure C: is display in the Look in field
3. Click on the Find button
4. Select all the result findings, right click on them and select the Properties… option from the walkout menu.
5. Click on the Security tab, then the Permission button on the dialog box to show the access permissions on those system files.



Restrict NULL Sections

Null user is the "ghost" in one's network. It could not be viewed in the User Manager GUI. The username and the password are both the null character. This account is used by the local system account to connect to remote systems.

The null users are member of the Everyone group without any credentials. Hackers could establish a null session connection to one's network and gather user account and group information from the domain controller and other information from the member-hosts of the network. The null session could even allow hackers to gain access to folders and files.

The Windows NT registry can be modified to prevent null session leaking internal SAM database information. This following must be made on all PDCs (primary domain controller).

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

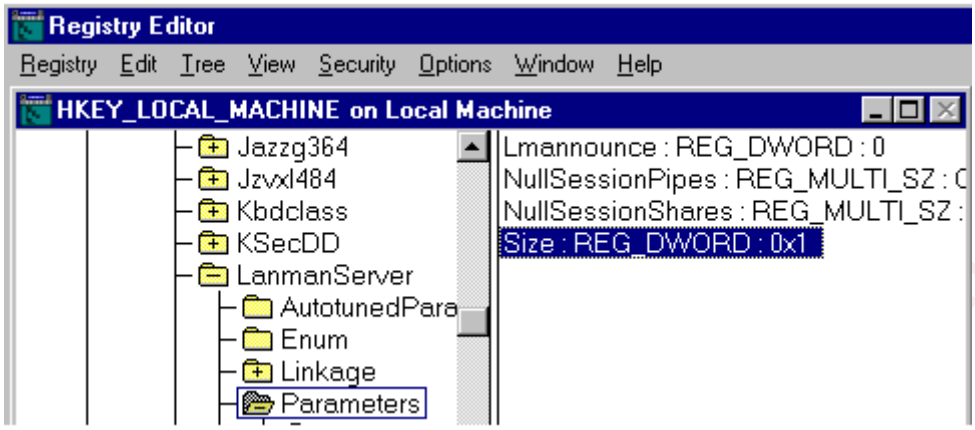
This RestrictAnonymous value is the same value on other hosts to prevent folder and printer shared names be listed by anonymous remote users.

There are two other registry key settings govern the access of the null session access to shared folders. The built-in System account and certain applications might need to use null sessions to access shares. Careful examination of the implications of turning off null session should be considered before implementation.

TestrictNullSessAccess registry key setting controls the on/off of the null session share access. When the value of this setting is 1, then null session users cannot access any shares. When the value of this setting is 0, then null session users can access any folder or printer shared to the Everyone group.

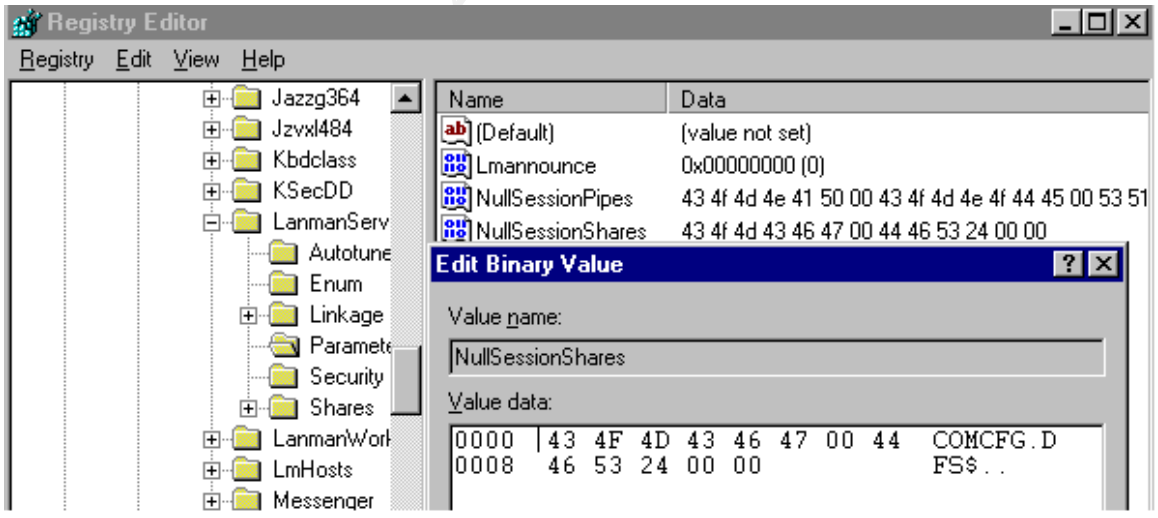
To restrict all null session access to all shares folders and printers, ensure the following registry key is present and set as the following.

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



Setting RestrictNullSessAccess to 1, it causes null session users cannot access shared folders and printers. This might prevent some application and services from working correctly. However, exceptions to this rule can be made by adding the desired shares in the NullSessionShare registry setting. The NullSessionShare value lists exceptions to the rule of denying anonymous user access when RestrictNUllSessAccess is set to 1. When restrictNullSessAccess is set to 0, then NullSessionShares is ignored.

Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Services\LanmanServer\Parameters
Value Name: NullSessionShares
Value Type: REG_MULTI_SZ
Value Data: <one or more Sharenames>



Please note that <one or more sharenames> should be just the name of the share, but not the explicit UNC path to that share.

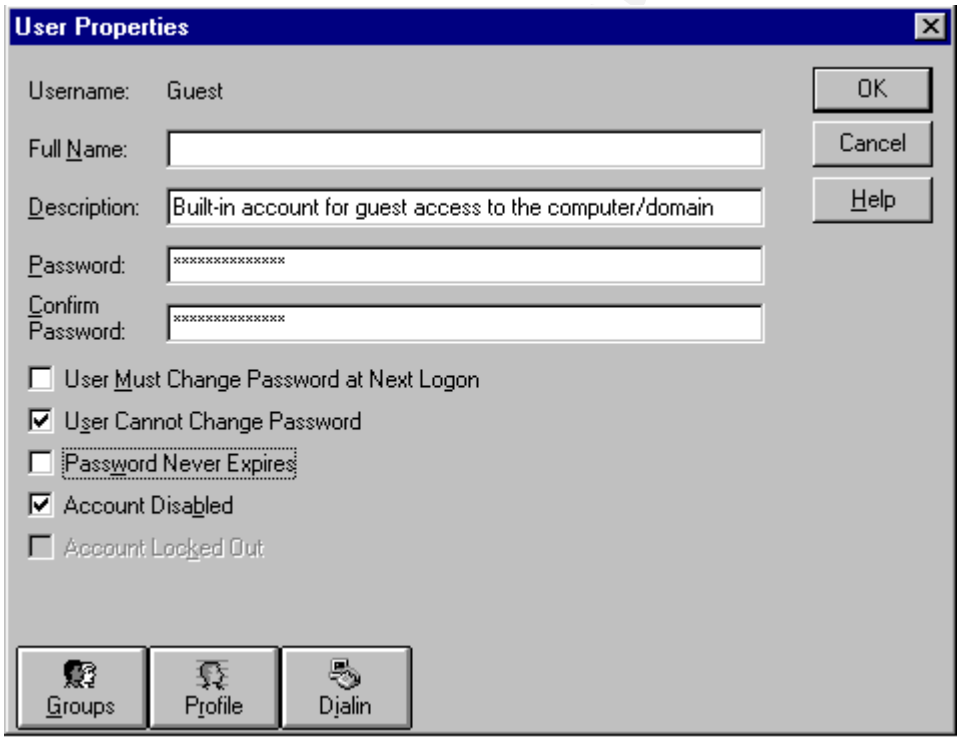
Built-in Account Management

Every Windows NT operating system has two built-in accounts, the Guest account and the Administrator account. These two accounts could not be removed from the system. On Windows NT Workstation, the Guest account is enabled by default; on Windows NT server, the Guest account is disabled by default. Because these two accounts are built-in and known, hackers will also attempt to break into the system by using these two accounts.

To prevent hackers attack the system by using the Guest account, ensure that the Guest accounts on the Windows NT Workstation and Windows NT Server are disabled, the password field is not blank, and the password Never Expires option is unchecked.

To check the Guest account setting

1. Launch the user manager or domain user manager from the Start > Programs > Administrative tools (Common)
2. Double click on the Guest account from the existing account list



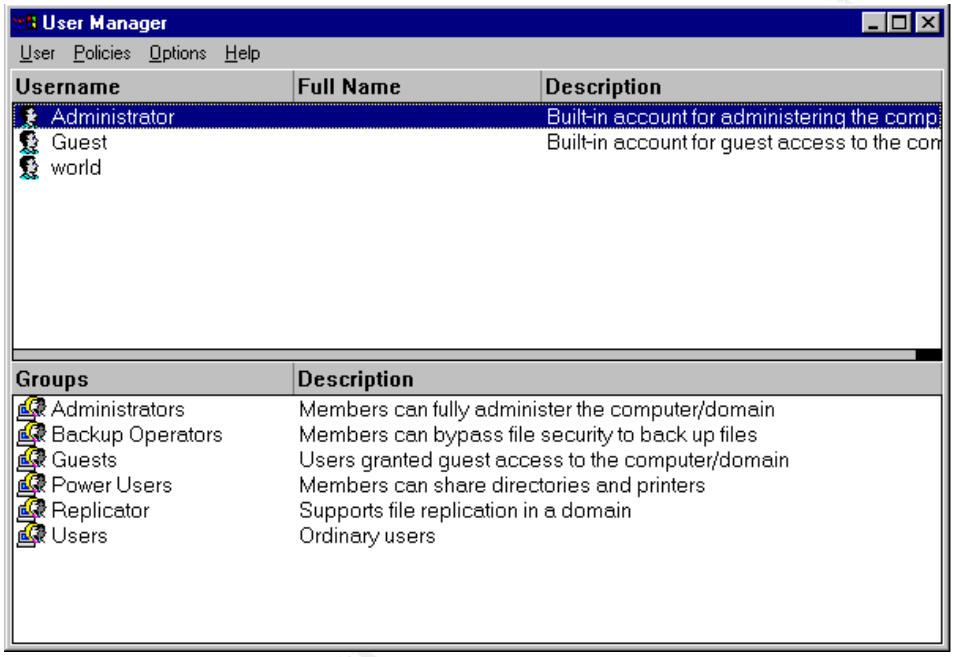
The built-in Administrator account is also the target for cracking due to its power and inability to be locked out by bad logon attempts. Administrators must be diligent in choosing very long complex passwords with at least on extended ASCII characters.

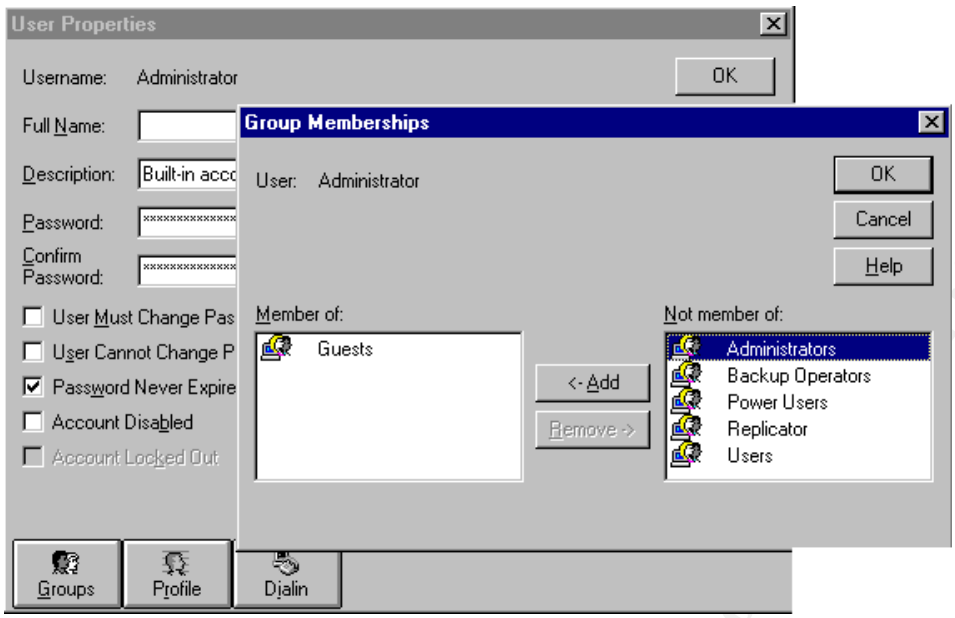
The built-in Administrator should be renamed. Ensure the description field for the account has been removed also. After renaming the built-in Administrator account, copy

this account and name the copy “Administrator”. The copied account should have no significant user rights, permissions or group memberships; make sure to remove it from the Administrators and Domain Admins groups; make sure to log on with the account at least once to make it appear active. The password for the honeypot account should be non-trivial but guessable. The Password Never Expire option should be set for this Administrator honeypot account.

To check the setting on the Administrator accounts

1. Launch the User Manager or Domain User Manager from the Start > Programs > administrative tools (Common)
2. Double click on the Administrator (This account is the honeypot account.)





In the User Manager screenshot, it shows that the built-in administrator has been renamed to world and the description has been removed also.

Secure SAM Database

By default, all user MD4 hashes of users' passwords and LanManager are stored in the Seucrity Account Manager (SAM) database. Utilities such as L0phtCrack can extract these password hashes in format suitable for cracking. The passwords in SAM database should be encrypted to prevent utilities from extract passwords from the SAM database.

With Service Pack 3 or later, the SAM can be encrypted with the SYSKEY.exe. The utility generates a 128-bit random key with which to encrypt the password hash in the SAM database. The random key is then encrypted with the system key. The system key holds the key to unlock the SAM database and it should be protected accordingly.

The System Key could be stored in three different ways according to the network environments' security level.

1. Hide the System key within the system itself with a "complex obscuring functions" to conceal it. This method should only be used in a secured computing environment, System key repository is local, and could be compromised later.

2. Stored on a floppy disk, this disk must be present whenever the system is rebooted. Due to the unreliability of floppy, it is recommended to make multiple copies of the disk. This method should be applied in a medium-security computing environment.

3. System Key can be generated (MD5) from a password up to 128 characters

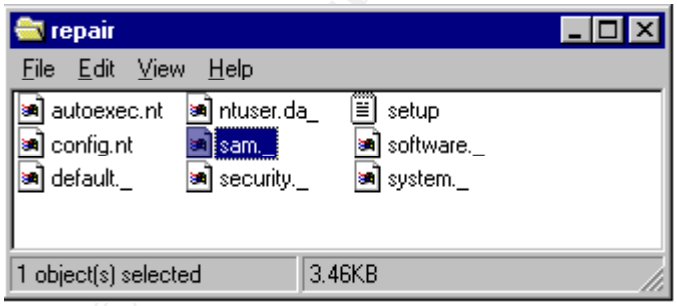
long. This password must be typed in by hand whenever the server reboots. The method should be applied in high-security computing environment, such the military, government agencies and etc.

The System Key must be used during the computer boot up to decrypt the passwords in the SAM database. Without the System Key, Windows NT system could not start.

The encryption of SAM database is irreversible. It is recommended to make a backup of the SAM database before encrypting it. The backup of the SAM database should be look in a safe, and only be used in the event that the System Key is not available.

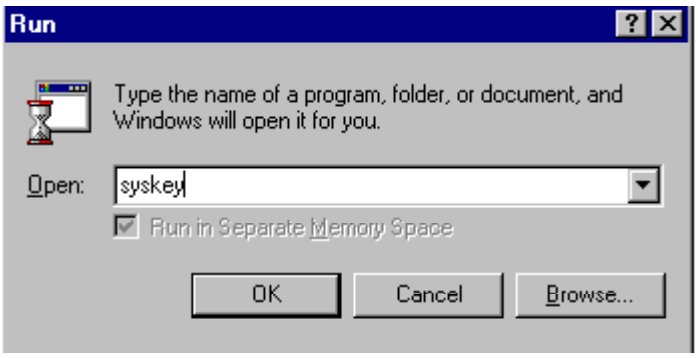
To backup a SAM database

1. Launch the rdisk /s by using Start > Run
2. Move to complete SAM database from \%SystemRoot%\repair directory onto a removable media or a secured server.
3. Make a few copy of the archived SAM database and store them in different secured location



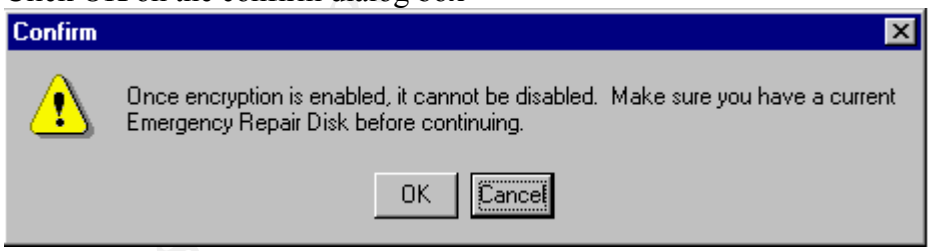
To use to SYSKEY.exe utility to secure passwords in the SAM database

1. Launch SYSKEY.exe from Start > Run

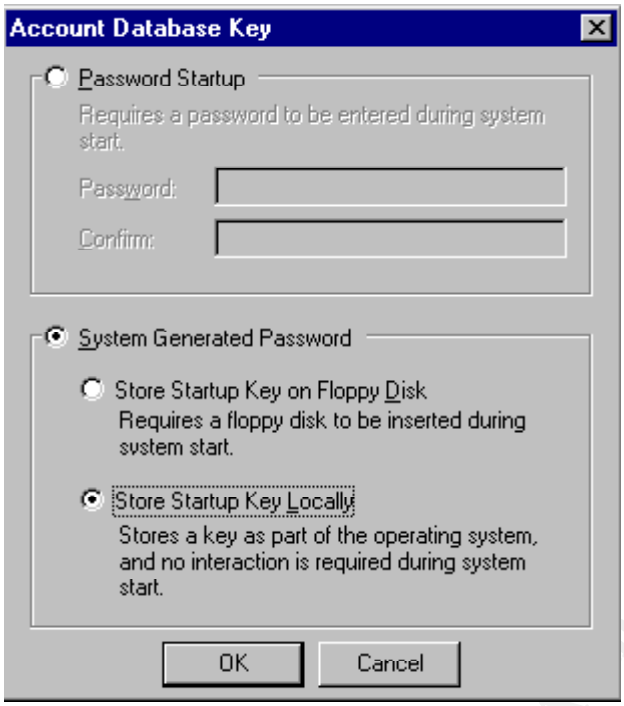


2. Select the "Encrypt Enabled" option and click OK

3. Click OK on the confirm dialog box



4. Select the appropriated option to store the System Key



Configuring the Event Logs

Administrators can track the security violations, application log, and system log in a system by using the EventView tool. It is crucial to configure the event logs before enabling any auditing. Event auditing writes events to the event logs and can cause the log to fill up the Boot partition.

The System and Application logs are used for analyzing DoS attacks. The Application log contains messages from drivers and services. The Security log is the most important one. This log helps track changes to the security system and identifies any possible breaches to security.

The location of the log files in not configurable. Ensure that there is enough free space in the Boot partition for both the event log files and paging files. As a rule of thumb, placing addition paging files in other partitions if capable. The sum of total log files should not greater than the amount of free space after subtracting the size of all page files plus 50 Meg.

The sizes of event log files are largely depending upon one's system audit policy and the wrapping option settings. The wrapping options are Overwrite Events as Needed, Overwrite Events Older than # days, and Do Not Overwrite Events (Clear Log Manually).

Overwrite Events as Needed
This option should never be used. This option allows the intruder to flush the log

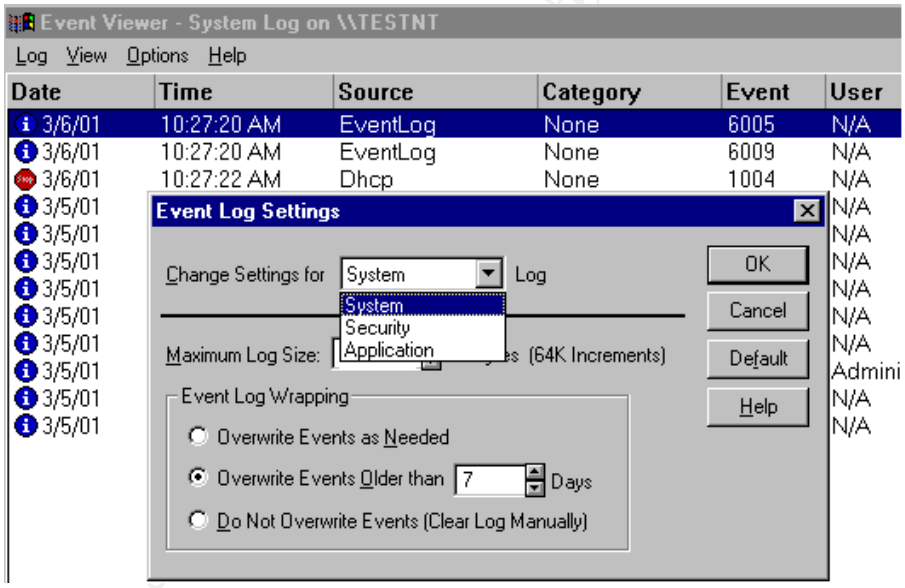
file with meaningless events. The intruder can launch an event generator to create meaningless or fault entries to flushing out the entries, which recorded the original intruder access events.

Overwrite Events Older than # days
This option is the best choice in medium-security network environment. The number of days set should be corresponding to the log's backup/export schedule. The log file size should be the average log file size times 1.50 to prevent situation where a log fills its capacity before it has been exported to a tape.

Do Not Overwrite Events (Clear Log Manually)
This option is usually applied in very high security environment. The option requires the event log files to be manually cleared. This option normally accompany with the CrashOnAuditFail registry setting.

To check the current event log file configuration

1. Launch the Event Viewer from Start > Program > Administrative Tools (Common)
2. Go to Log > Log Settings.



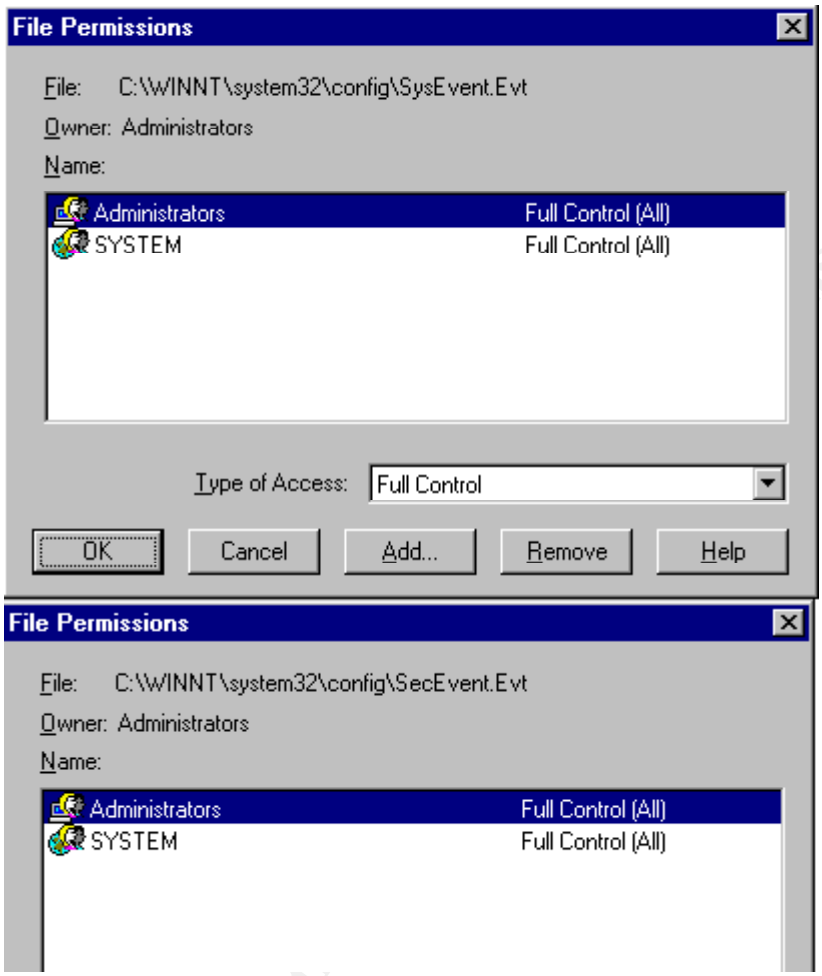
The restricted access permission should be assigned to the event log files. The System account and the local Administrations group should be assigned Full Control of the event log files.

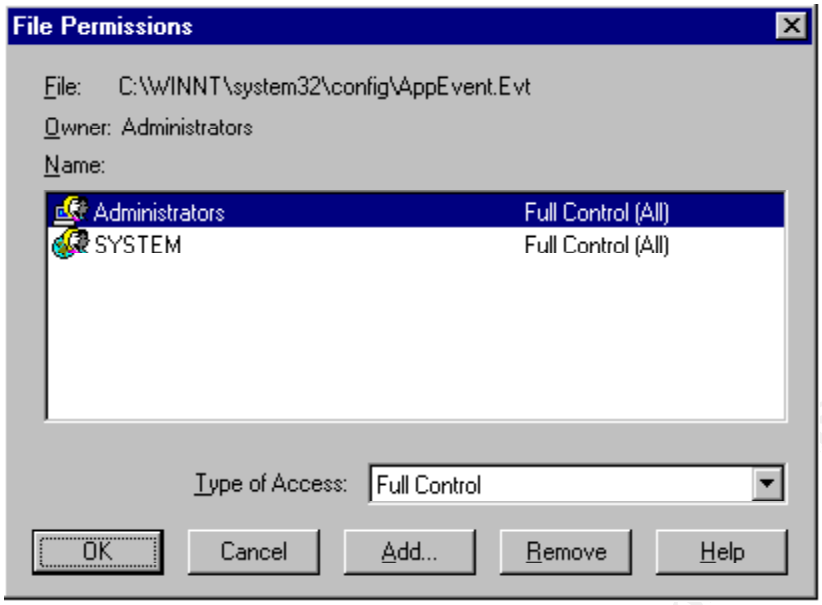
To check the NTFS setting on the log file

1. Navigate to \%systemRoot%\system32\conig
2. Select the SysEvent.evt, SecEvent.evt, and AppEvent.evt
3. Right click on each of these files and select the Properties … option from the

walkout menu, click on the Permissions button

The permissions settings on these files should look similar to the followings:





Audit Policy Configuration

Windows NT has extensive built-in auditing. It is broken down into seven different categories. Auditing can be enabled on all or some of these categories success or/and failure attempts.

Logon and Logoff
These events record a single logon or/and logoff attempt, regardless successful or not. The event indicates what type of logon was requested.

File and Object Access
These events record both successful or/and failed access attempt to protect files and objects.

Use of User Rights
These events record both successful or/and failed attempts to use privileges.

User and Group Management
These events record all users account modifications. These events provide help administrator to figure out what account the intruder created after a system has been invaded.

Security Policy Changes
These events record high-level change to security policy database.

Restart, Shutdown, and System
These events record restart or shutdown event of a system.

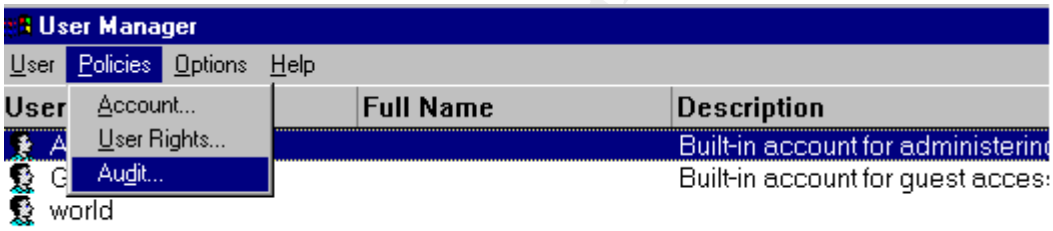
Process Tracking
These events record detailed tracking information for certain events. These includes program activation, some forms of handle duplication and etc.

There are no standard formulas on deciding what type of audit categories should be enabled. Keep in mind when you are deciding what categories you need to audit, the more auditing you do, the more CPU and disk spaces are used.

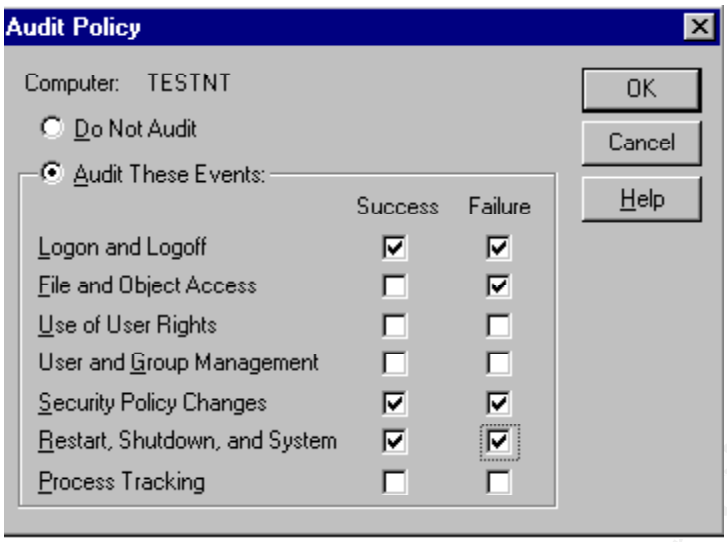
I will go step-by-step and explain the most popular auditing configuration from the Department of the Navy. This auditing configuration policy used here should only be used as a guideline.

To audit the system

1. Launch User Manager for the Start > Programs > Administrative Tools (Common)
2. Select the Audit… option from the Policies menu

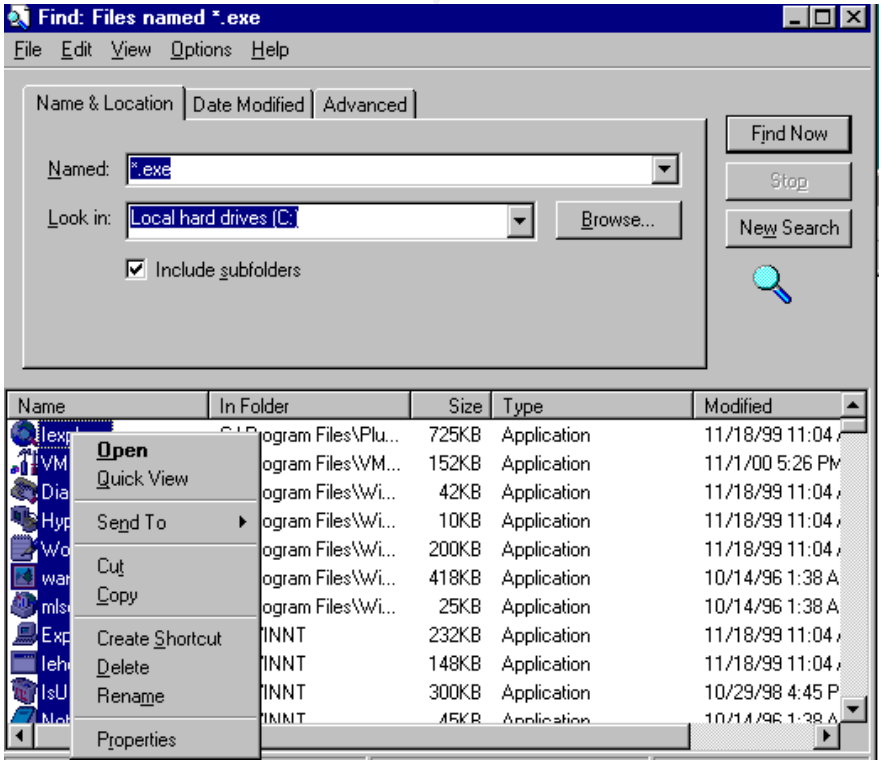


3. Check the Audit These Events option on the Audit Policy dialog. A window with the following options to audit on success or failure will appear. File and object access must be enabled to audit on directory/file and printers. Auditing on failed logins allows the administrator to check what account has been use for that attempt and at what time. Most of system uses are legitimated users, auditing on successes for File and Object Access will fill the logs rapidly. So, success for File and Object access should not be enabled.

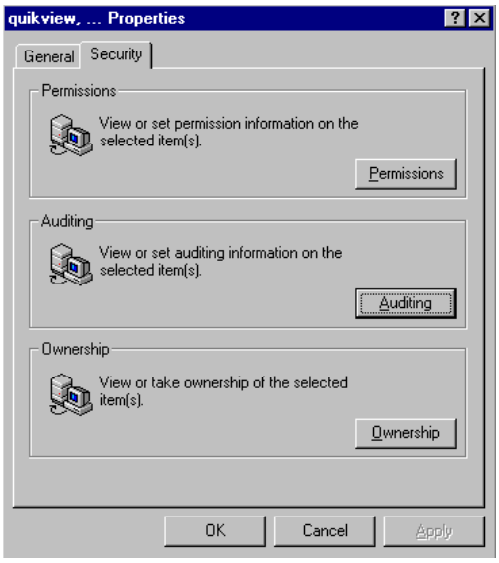


4. Auditing all executables in Boot partition, especially the \%RootSystem%\ directory. Adding the Everyone to the list, and then choose to audit failures for write and delete, and successes and failures for changes Permissions and Take Ownership. Executables in the Boot partition are either copied from the Windows NT CD Rom or from Service Packs. Those files are crucial to the system itself.

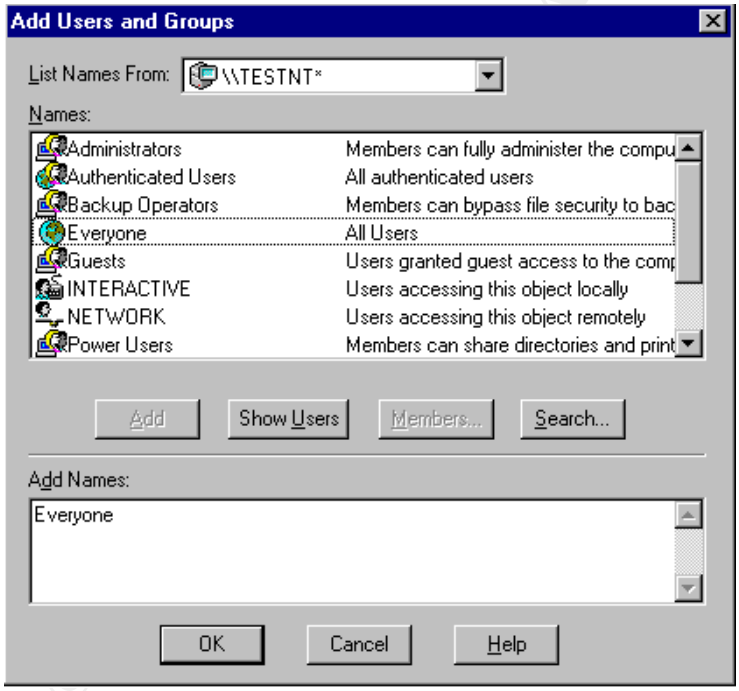
   4.1 Gather files and select the Prosperities… option



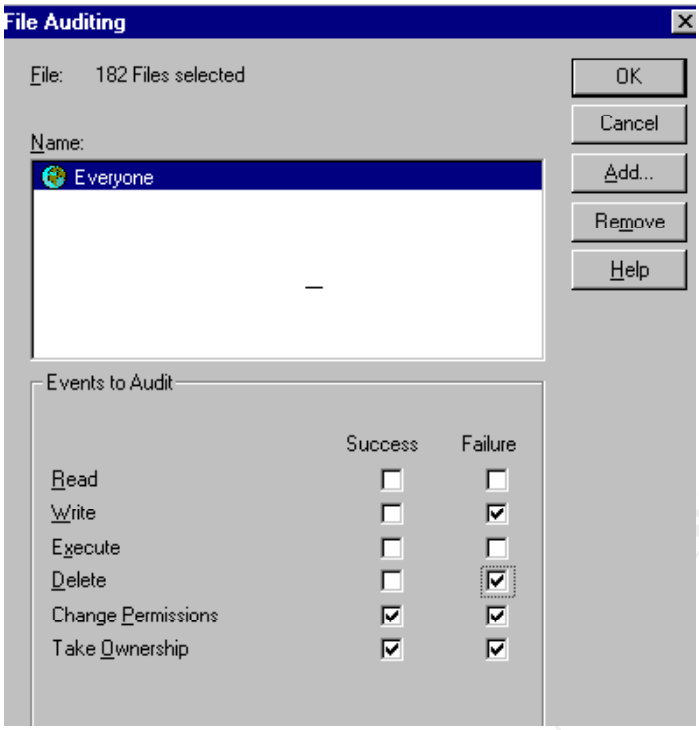
   4.2 Click the Security tab, and then select the Auditing options



4.3. Click the Add… button on the File Auditing window, then select the Everyone from the Names: listing and then add Everyone to the Add Names list

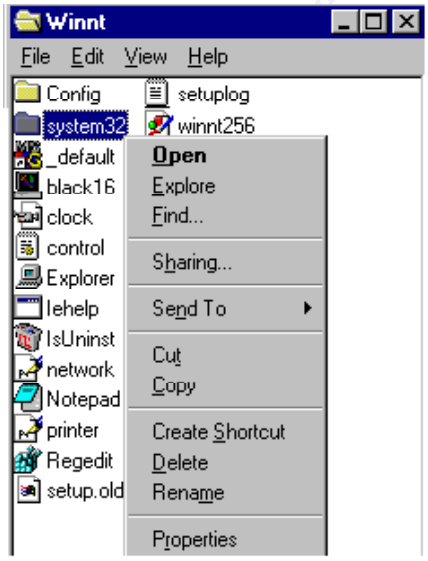


4.3. Enable file audit failures for Write and Delete, and successes and failures for Change Permissions and Take Ownership

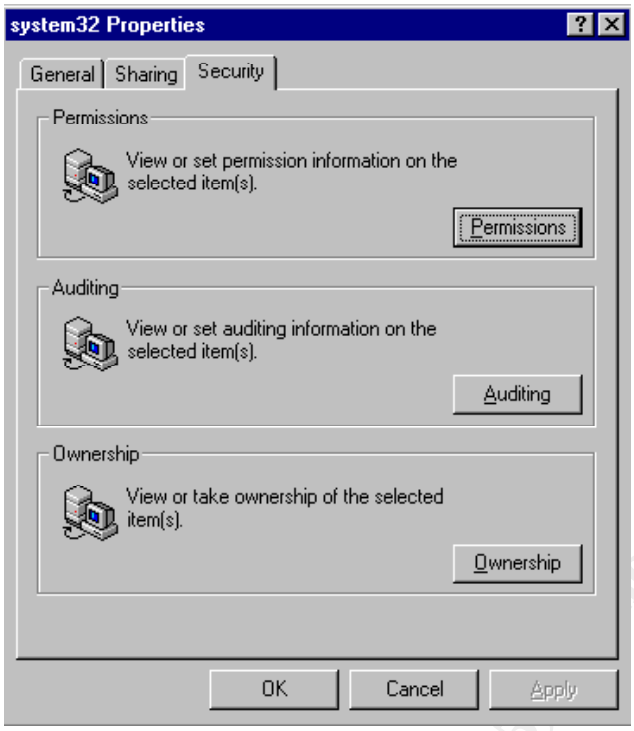


5. Auditing the \%RootSystem%\system32 and \%RootSystem%\repair will monitor system repair data integrity and security information. Applying audit services to directory should be one by one.

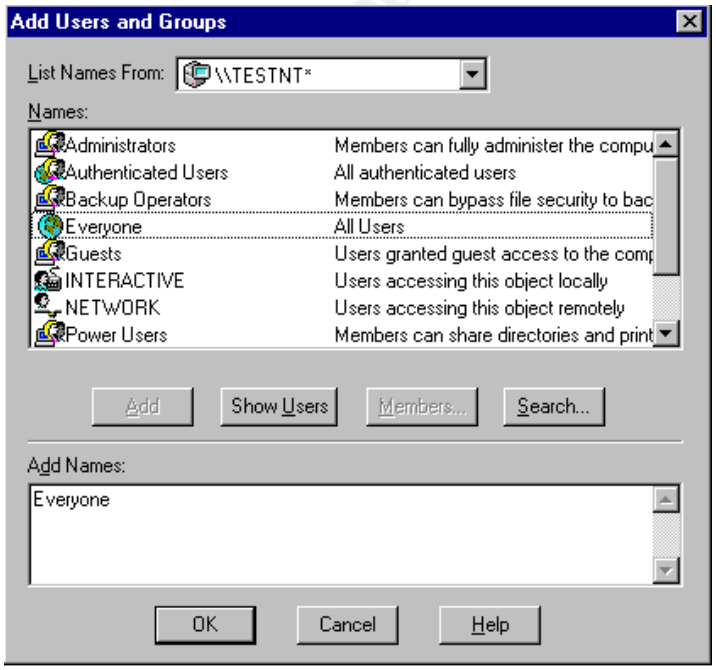
   5.1.1. Navigate to \%RootSystem%\system32 directory and select the Properties … option from the right click walkout menu



   5.1.2. Click at the Security tab and then click at the Auditing … button on the system 32 Properties window

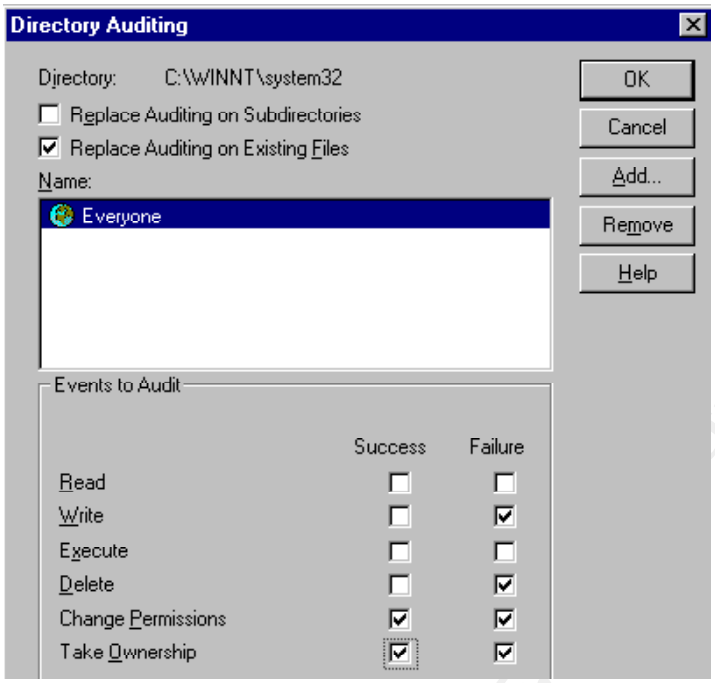


5.1.3. Click at the Add… button on the Directory Auditing window, add Everyone from the Names: list to the Add Names: list, then click in the Add Users and Group window

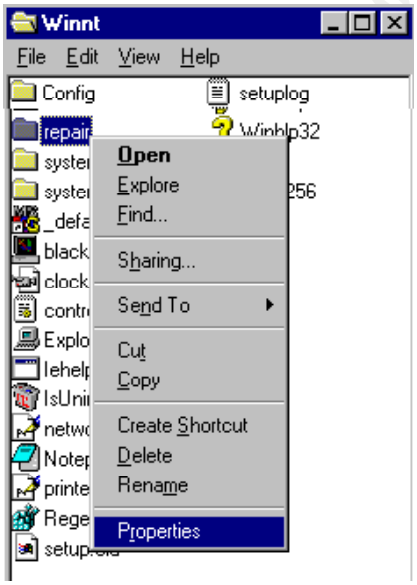


5.1.4. Enable auditing failures for Write and Delete, and Successes and failures for Change Permissions and Take Ownership, then Click on the Directory

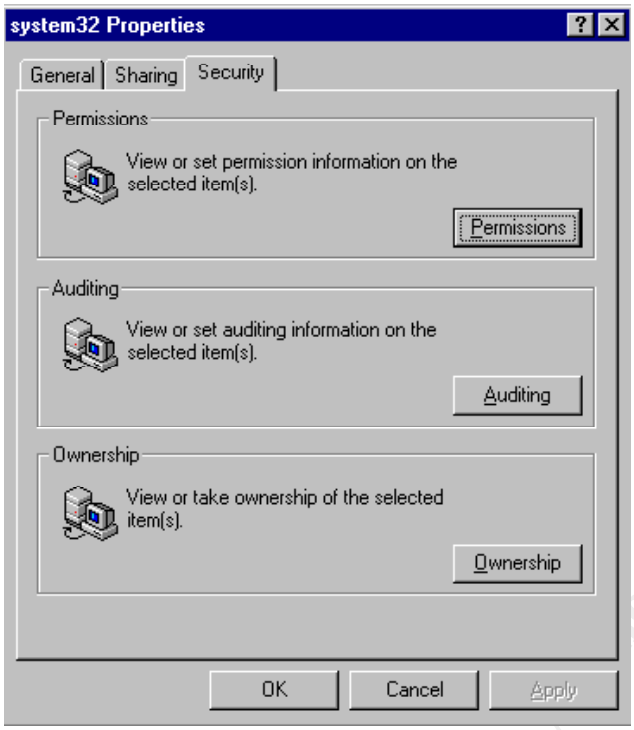
Auditing window



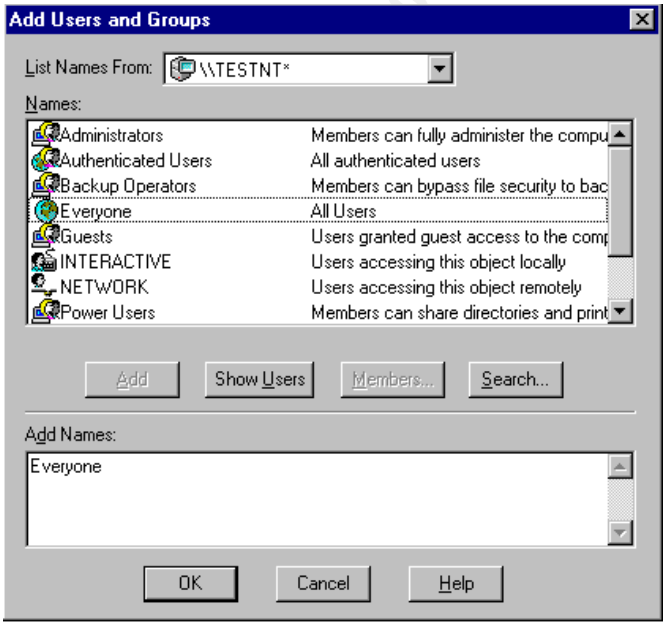
5.2.1. Navigate to \%RootSystem%\repair directory and select the Properties … option from the right click walkout menu



5.2.2. Click at the Security tab and then click at the Auditing … button on the System 32 Properties window



5.2.3. Click at the Add… button on the Directory Auditing window, add Everyone from the Names: list to the Add Names: list, then click in the Add Users and Group window



5.2.4. Enable auditing failures for Write and Delete, and Successes and failures for Change Permissions and Take Ownership, and then click on the Directory Auditing window

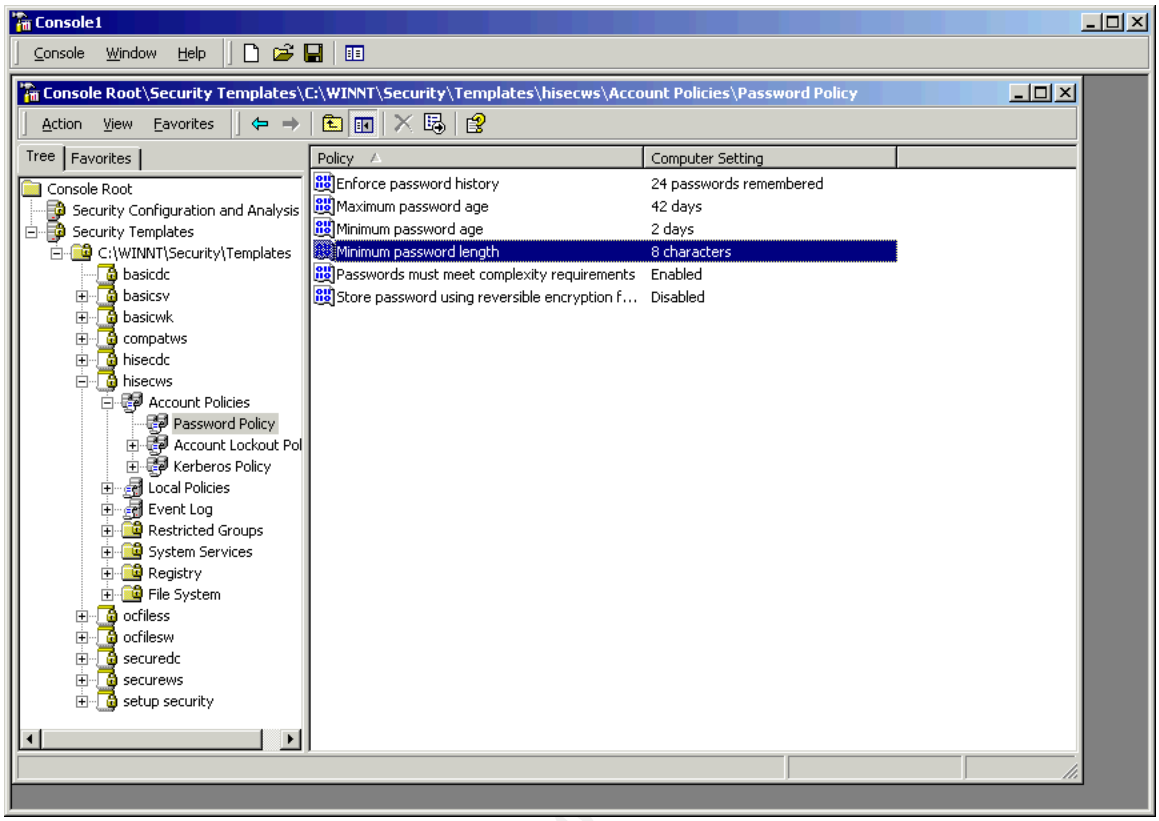
Microsoft Security Configuration Editor (SCE)

Microsoft Security Configuration Editor is a snap-in to the Microsoft Management Console (MMC), which is an essential tool for system administrator in Windows 2000. SCE provides a common place to configure system security prospects. The security prospects include Password Policy/Password Strength, appropriate NTFS permissions, registry key settings, Event Log settings and etc.

SEC is an administrator crucial tool from Microsoft. SEC works on template base. It can define a security template, compare a selected template against the local machine's current settings and generate a comparison result, apply a template to a system, exact current host configurations data and generates a template. It provides the simplest means for administrator to manage security settings for complex Windows NT network. The SEC requires Service Pack 4 or up.

SEC is a must to have tool to audit a Windows NT system. It exports the host's current security configuration to a new template. Auditors can exact data from the template and compare it against the documented security policies.

SEC could be downloaded for free from Microsoft's FTP site "ftp://ftp.microsoft.com/bussys/winnt/winnt-pulic/tools/scm/". The downloaded package includes SEC and MMC. Here is a screenshot on password policy settings.



Work Cited

Department of the Navy. Secure Windows NT Installation and configuration Guide http://www.rito.com/nt/ntsec/navy

Microsoft Press. Microsoft Windows NT server Resource Kit version 4.0, Supplement One, Microsoft Corporation, 1997

SANS Institute. Windows Security Step by Step, 2000, The SANS Institute, 2000.

Wendt Carla. Auditing Review. Washing DC: The SANS Institute.

Perkings, Strebe, Chellis. MCSE NT Wrokstation Study Guide. California: Sybex, 1997

Microsoft Corporation. MSDN Online Library, http://www.msdn.microsoft.com/library/default.asp, Microsoft Corporation, 2001

Do, George. GCNT Certification Submission, http://www.sans.org/giactc/gcnt.htm Analyst Number 0061 GeorgeDo.doc