Global Information Assurance Certification Paper

COMMAND AUDIT POLICY

By
Nancy L. Roberts
SANS ID- roberts005

GIAC NT

Practical Assignment for Mary Washington College
Securing Windows NT
April 2, 2001

Executive Summary:

This practical is submitted to fulfill the SANS requirement for Securing Windows NT. After completing the required readings for this course, it was easy to identify a weakness within our command. A formalized Audit Policy was not in place that provided a comprehensive procedure for implementing **WHAT** is required to be audited and a procedure on **HOW-TO** effectively monitor the audit logs and LAN configuration.

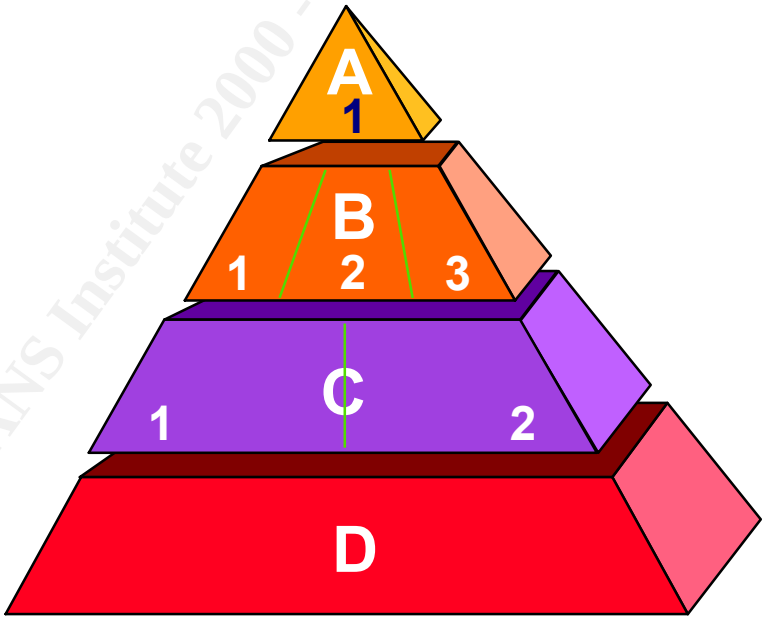
Michael J. Moore provides information similar to that presented in the following paper in his work "Issues with Auditing Windows NT4.0 Server". [(1)]
I have chosen to answer the practical requirements by developing an Audit Policy Procedure that could be implemented throughout my area of responsibility, 108 facilities. To support this focus Public Law, Department of Defense (DOD) , Department of Navy (DON), and Secure Windows NT Installation and Configuration are used to develop a definitive Audit procedure. Supporting documentation from SANS practicals located at http://www.sans.org/giactc/gcnt.htm, SANS Institute Windows NT Security Step-by-Step, and other pertinent documentation were also used.

This Audit Procedure assumes that a successful installation of Windows NT 4.0 with Service Pack 6a has been completed for a Sensitive But Unclassified Network (SBU) in a single domain, which has been determined to be at a low to moderate level of risk. This Audit Procedure is designed for implementation on a Primary Domain Controller. Settings would be slightly different on NT Workstations or Member Servers. Individual configurations are beyond the scope of this practical.

Introduction:

Public Law and DOD regulation requires that every system be accredited. Accreditation is a multi-phased process of determining the level of risk a system is exposed to, the level of trust that the system design and implementation provides, the classification level of information processed, and the classification and access levels granted to the personnel with access to the system. The process for Accreditation is beyond the scope of this practical, however, the requirement to Accredit a system is the legal basis for Auditing systems within DOD. The Level of Trust defined in the Accreditation is partially based on the Audit Policy established for the system.

The required Levels of Trust established by DOD varies based on the design and implementation of the computer systems. These levels are categorized as Trusted Computing Base (TCB). The levels of trust are described in the National Computer Security Center (NCSC) documents, commonly referred to as the "Rainbow Series," so named for the different colored covers given to each of the various books. The different TCB designations are rated from levels "A" to "D" with "A" being the most secure level and each level being divided into categories of trust designated by numerical subcategories. The numerical designations run from 1 at the lower level to 3 at the higher level for that specific category. A "C2" level of trust is required for an SBU LAN such as the one at many of our commands and the subject of this Audit Procedure.



TCB EVALUATION DIVISION AS SPECIFIED BY THE ORANGE BOOK[2]

Windows NT 4.0 was designed by Microsoft to meet the C2 level of trust as defined by NCSC. There are 4 basic elements that must be met in the design and implementation to obtain the C2 rating: Discretionary Access

Controls, Identification and Authentication, Audit and Object Reuse. All 4 of these elements are present in Windows NT 4.0. However, in the default installation Auditing is not configured at the C2 level. After the NT installation is complete, Auditing must be turned on and auditing parameters set.

This paper walks through the steps necessary to manually configure accounts to provide a baseline upon which to audit, steps to implement auditing, an introduction to Registry basics and Department of Navy (DON) recommended secure configuration .inf template file for use with SCM. Additionally, a set of utilities has been developed to assist the administrator or auditor to capture audit statistics and event logs for use in troubleshooting system problems, documenting application events, as well as historical records for forensic evidence. The following Audit Procedure is compliant with applicable Public Law and DOD regulation and is based on the requirement established by the DON for Sensitive But Unclassified networks running Windows NT 4.0 in the Secure Windows NT Installation and Configuration Guide.

Identification and Authentication:

Prior to focusing on implementing the desired Audit Policy, Identification and Authentication of users must be configured. This will provide the access limitation for which Auditing can be configured to monitor.

The general rule for creating user accounts is the rule of “least privilege.” Least Privilege is the practice of allocating users and system operators the minimal permission necessary while adequate to allow accomplishment of their task assignments and responsibilities on the system.

The use of a user template in conjunction with effective use of Groups will aid the administrator in securely managing user accounts and will assist Administrators in defining Limited Privilege accounts. To begin this task, create a new user account with the Username TEMPLATE. Click Start, Programs, Administrator Tools (Common), User Manager for Domains. When the User Manager Screen Opens, Select the User Pull Down Menu and New User. Figure 1 displays the TEMPLATE account.

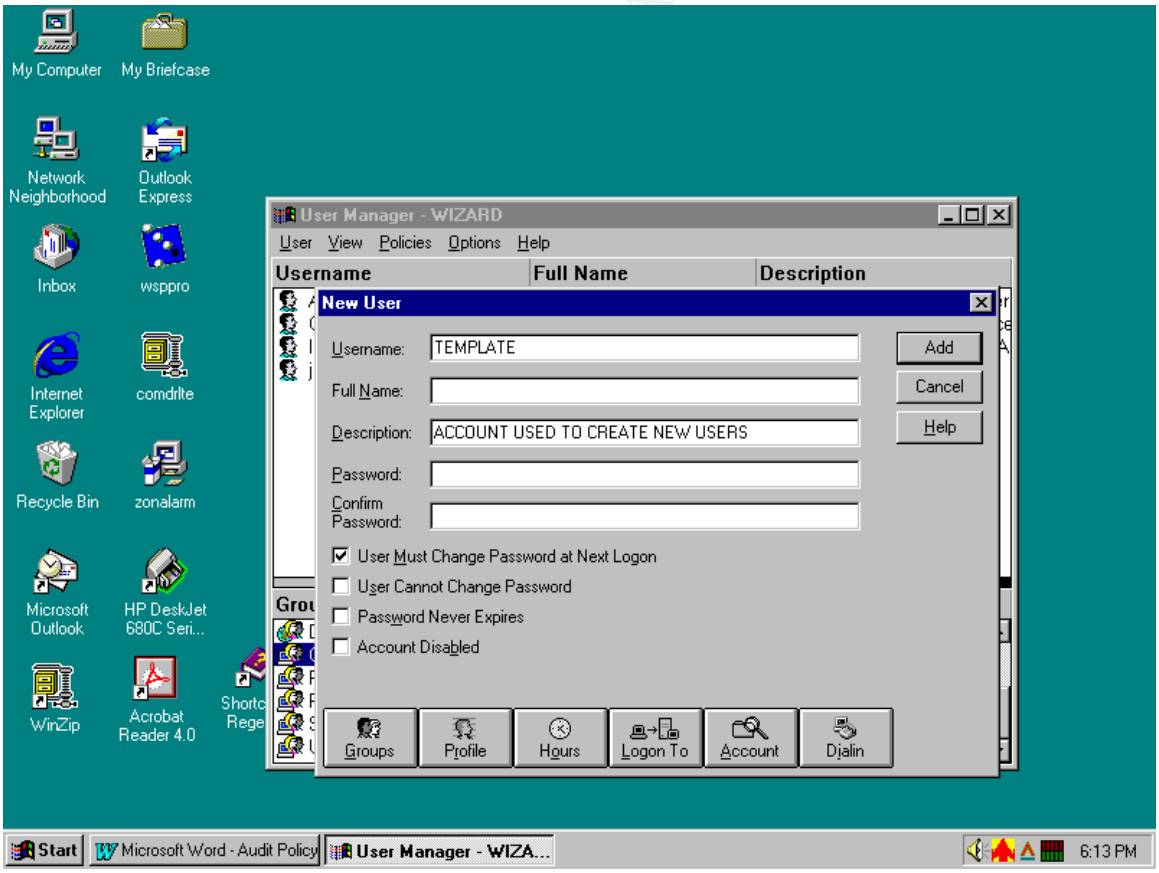


Figure 1.

Basic User Accounts restrictions is displayed in Figure 2. Accounts should be configured to require the user to change the password when they log on for the first time to ensure that the password is unique and the password is one that they can remember without having to write it down. (DON does not require computer generated random password on SBU Networks.) The original password created by the System Administrator or the Accounts Operator should be randomly selected. This password should not be used generically, i.e. do not select a password for the day or month that is used for all the account administration or modifications, creating new accounts or replacing forgotten passwords, etc.

In User Manager, select Policies, then Select Account, to specify defaults policies affecting all user accounts.

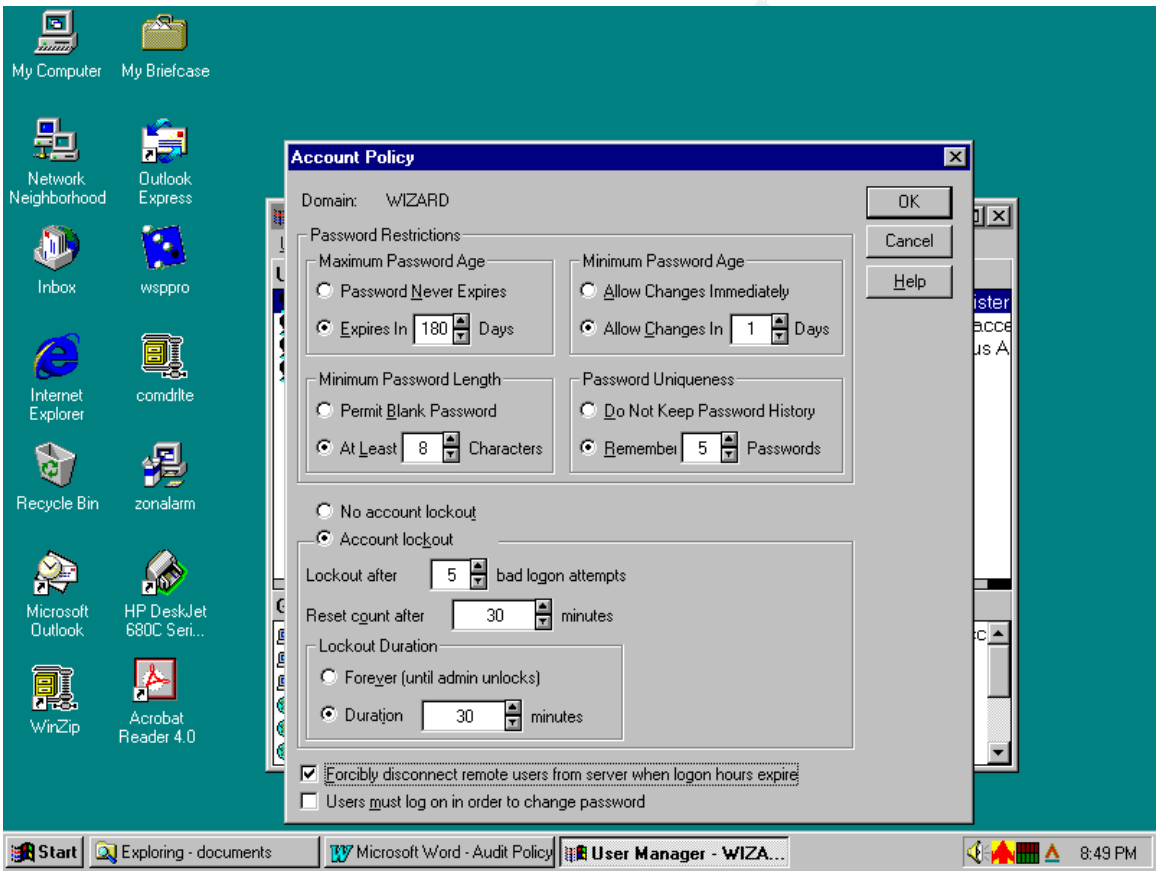


Figure 2.

DON Policy Minimums

Minimum Password Age	1
Maximum Password Age	180
Minimum Password Length	8
Password History	5
Lockout after X bad logon attempts	5

Lockout Duration	30
Forcibly disconnect remote users from server when logon hours expire	Select

However based on Industry Best Practice it is recommended that stronger restriction be placed on default user accounts.

Password Length	12-14
Lockout Duration	4 hours
Password History	10
Maximum Password Age	45-90
Lockout after X bad logon attempts	3

Password length should be set based on how long it would take to break the password with a cracking program such as L0phtcrack or Brutus. Best practice for Duration should provide the user and system administrator adequate time to determine that unauthorized access has been attempted, a more acceptable duration would be set to 4 hours. (3)

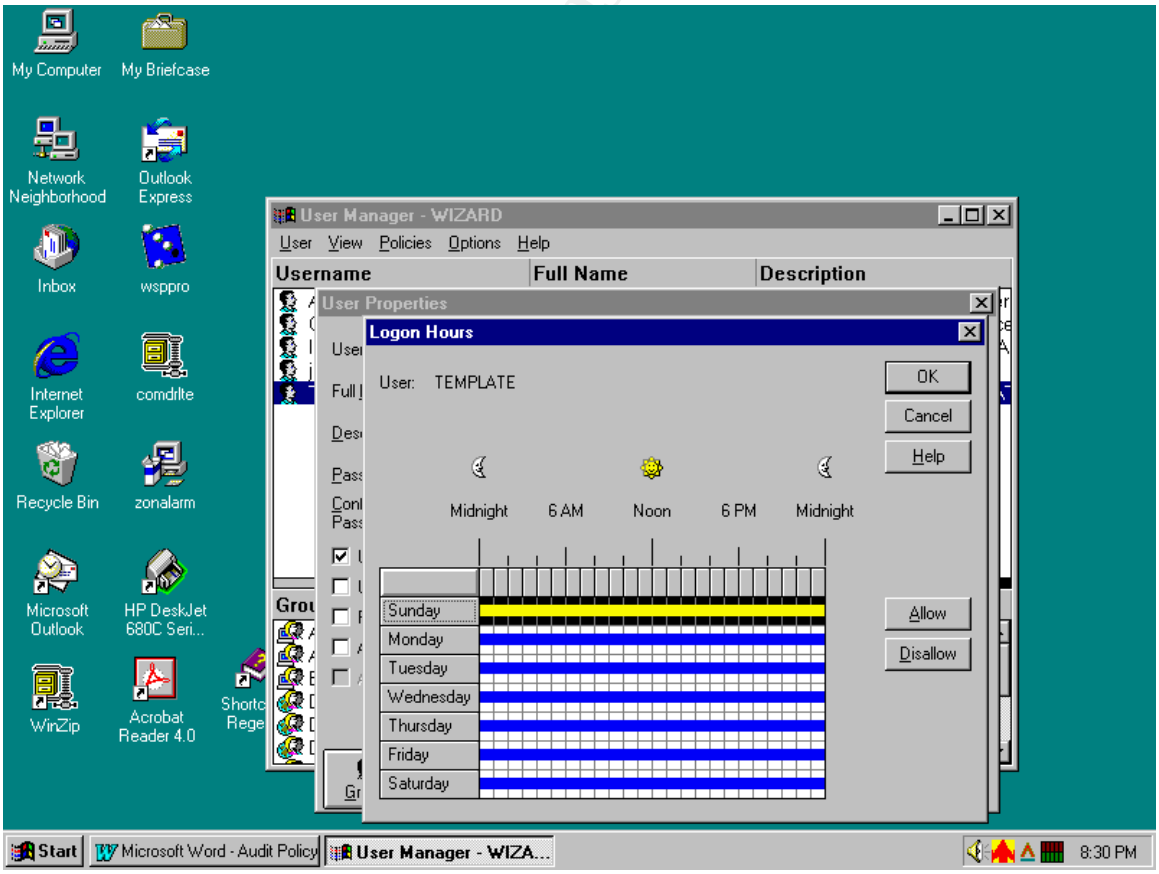


Figure 3.

Forced log out is required for all users within the command at least once everyday. This can be done in the User Manager, Hours screen. Figure 3, above displays the Hours screen from the TEMPLATE Account. Highlight the days, or times the user is not authorized access to the system. Only System Administrator accounts should be authorized 24/7 access to the system

Likewise remote Dial-in Access should also be restricted if the user is not required to perform off-site system access that would require them to dial in to the network. By default accounts are not authorized dial-in access, this can be verified on the Dial-in Screen under User Properties as displayed in Figure 4.

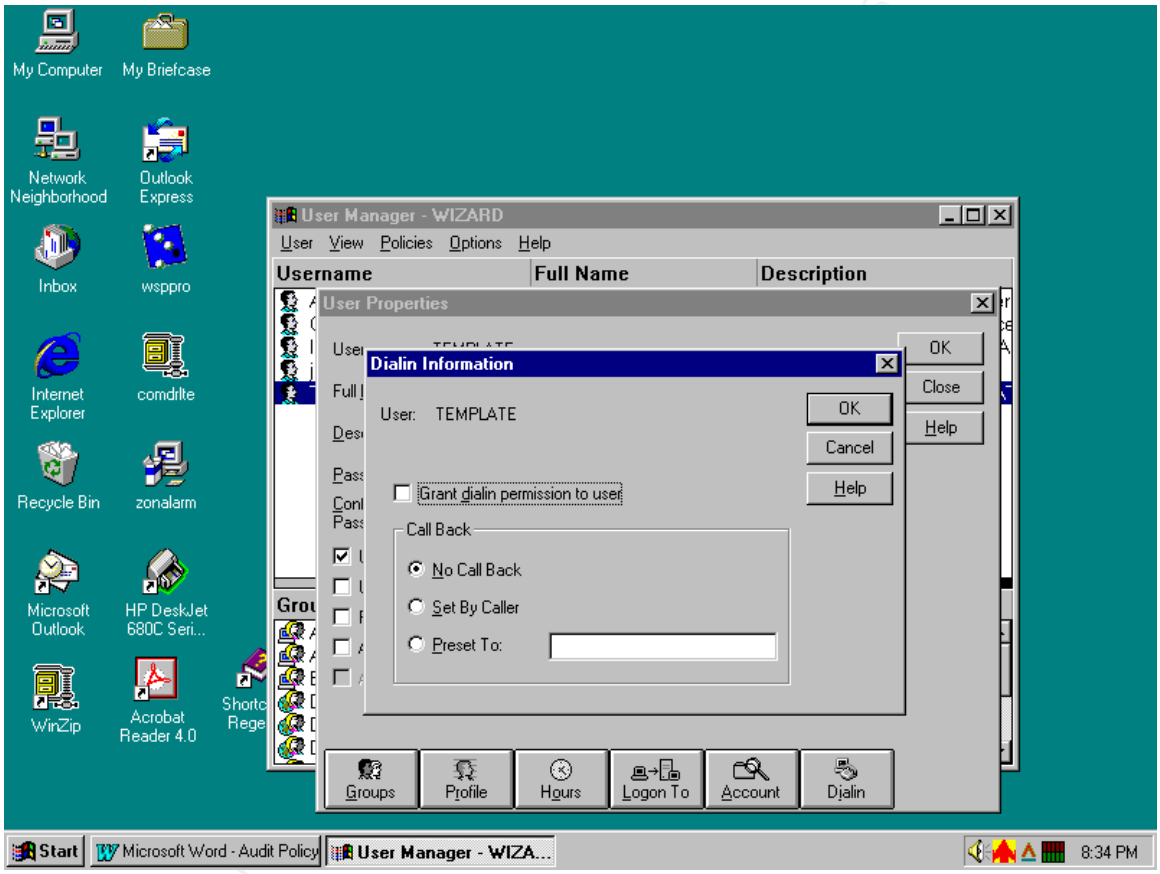


Figure 4.

Group Membership is then selected to provide additional permission required for the job function of the users account being created. The default Group Membership is Domain Users (see Figure 5). Select additional groups as required.

Note: The number of personnel assigned to the Administrator Group should be maintained at the lowest possible level while ensuring adequate backup for emergencies and managerial oversight. It is recommended that a Maximum of

3 accounts be assigned to the Administrator Group.

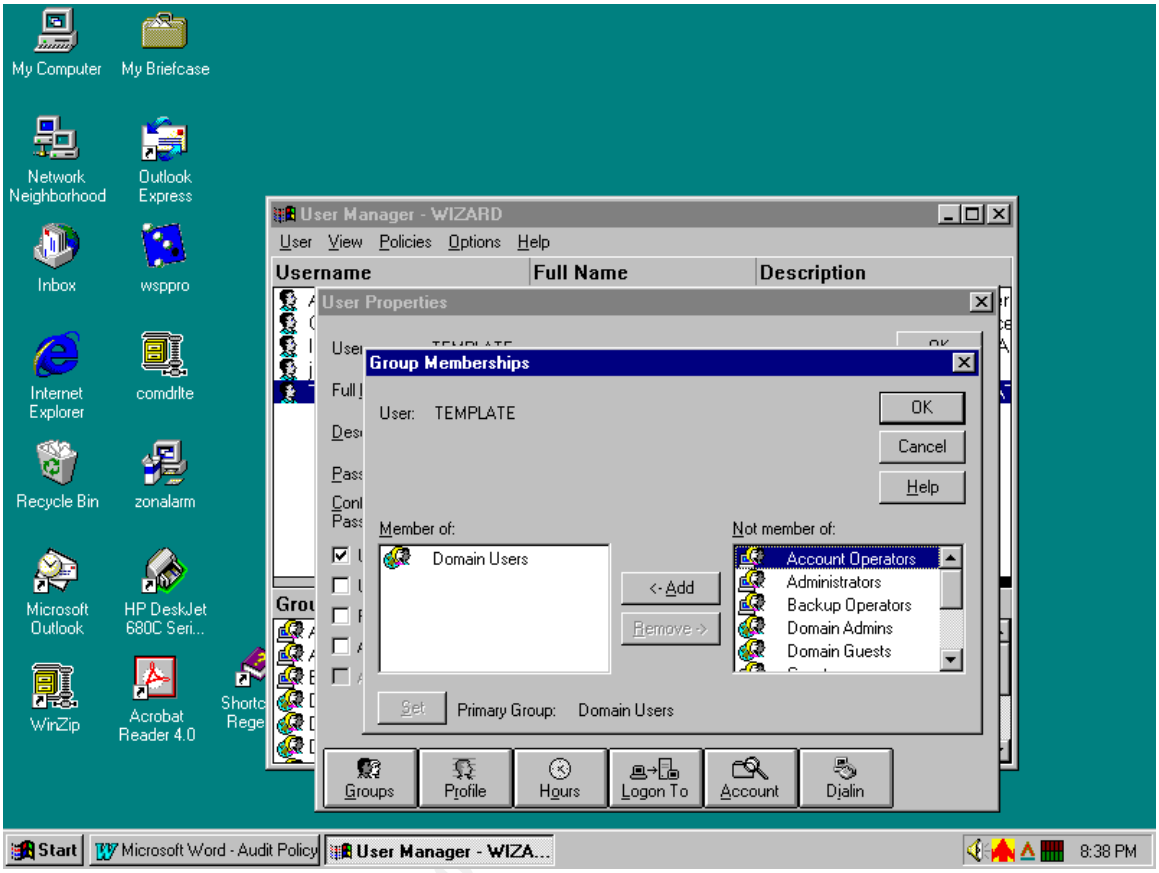


Figure 5.

WinNT provides several Default groups: Administrators, Guest, Everyone, Backup Operators, Account Operator, Domain Users, Domain Guests, Domain Admins, Printer Operators, Replicator, Server Operators and Users. The default groups make the task of creating new User accounts quicker and easier by providing template groups with the necessary permission to enable them to perform the specific functions as identified by the group name. Following this philosophy, the use of Groups can provide a more error-free method for the system Administrator to establish user accounts and assign the requisite permissions.

The Everyone default group is specifically prone to unauthorized access attempts. The Everyone Group provides access to literally “Everyone,” authenticated users, null sessions and unauthenticated users. DON C2 configuration requires the Everyone Group be restricted and not be granted access in a normal configurations. (Exceptions can be authorized by the Designated Approval Authority for the specific computer system on a case by case basis.) This Audit Policy follows the normal implementation without exceptions or waivers. Null Sessions and Unauthenticated users provide an

entry point for malicious users or malicious code[4]. An alternative to the Everyone Group is the group Authenticated Users.

Assigning the Users in to the Authenticated Users Group and assigning files, directories and resources permissions to the Authenticated Group instead of the Everyone Group will provide a greater degree of access control. If the facility has specific programs that require "null session" access that can not be reconfigured, the "Everyone" Group will have to be used. This requirement should be reported to the commands reporting senior and included in the Risk Assessment prior to system Accreditation.

The Authenticated User group is not displayed as a WinNT default and must be added. This is accomplished as depicted in Figure 6 below, Click Start, Programs, Administrator Tools (Common), User Manager for Domains. When the User Manager Screen Opens, Click on the Policies Pull Down Menu and select User Rights. Select Add, and Select Authenticated users.

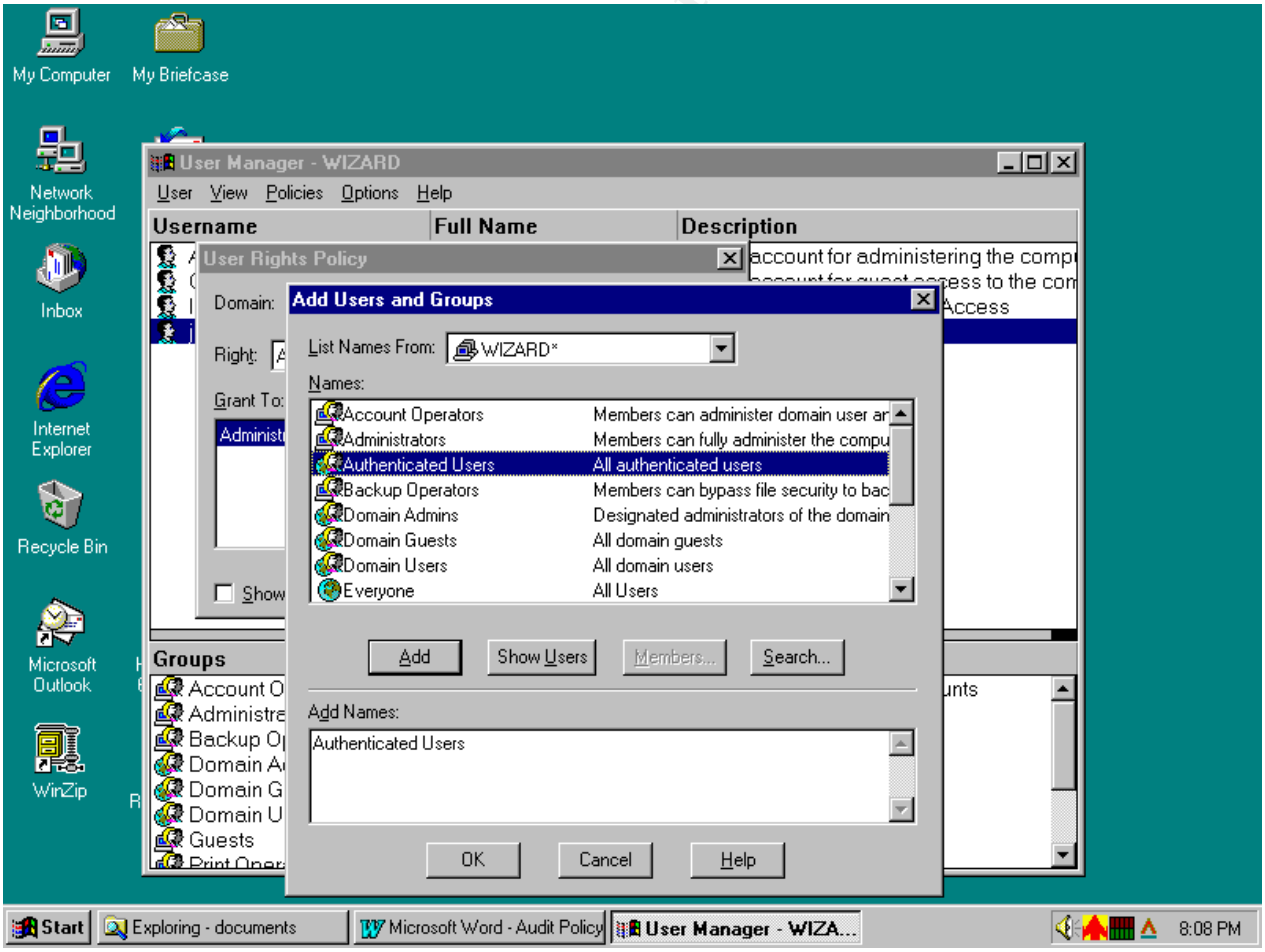


Figure 6.

Next, the Guest User Account must be modified to provide additional restrictions. This account is high on the list for unauthorized access by system attackers and crackers. The Guest Account is disabled by default in WinNT Server installations. Adding a password will require a more sophisticated level of attack in order to gain unauthorized access using the Guest Account.

From the User Manager for Domain screen, double click on the Guest Account, and enter and confirm a password, and ensure “Account Disabled” is selected, as display in Figure 7. The Guest password should then be written down and placed in a sealed envelope, and stored in a safe for emergency activation.

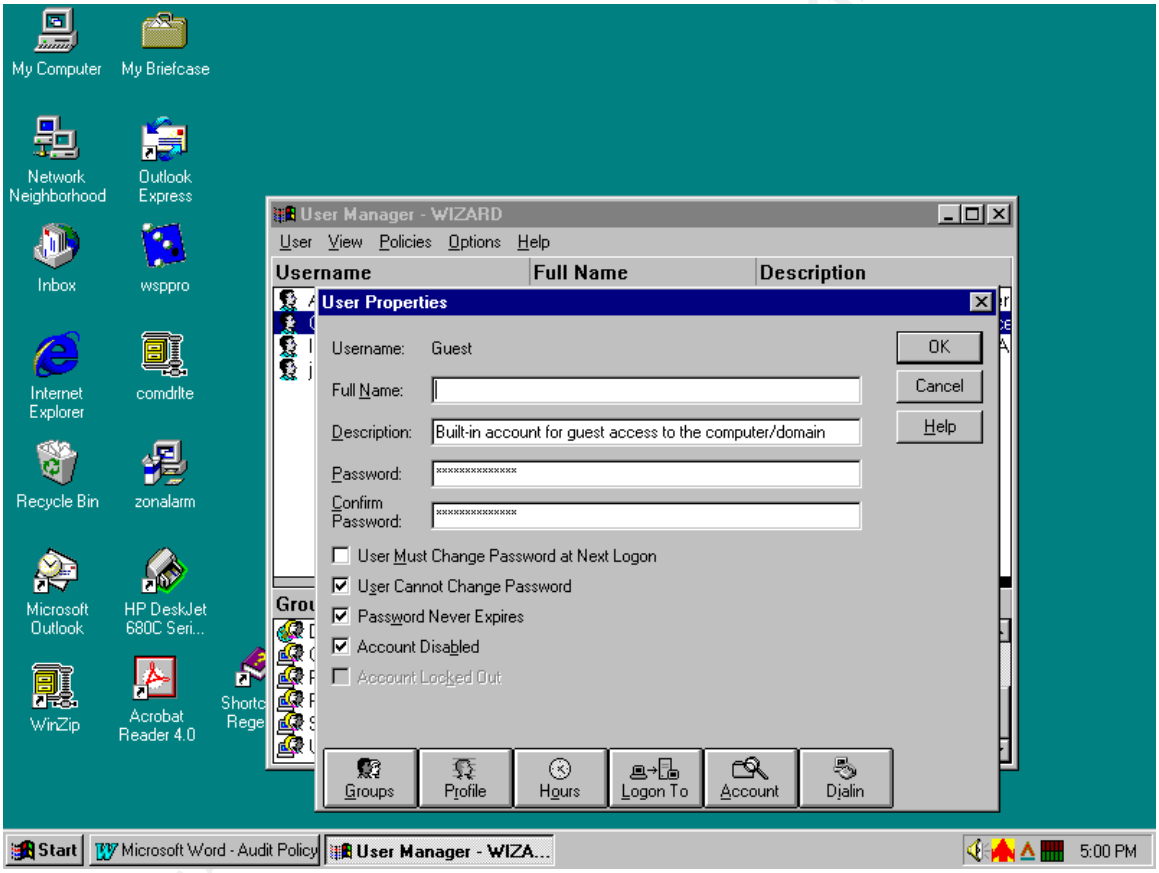


Figure 7.

Now that basic Identification and Authentication have been configured, Auditing must be configured.

Auditing:

The requirements used to establish an auditing policy by a facility is somewhat a subjective decision. Auditing is a teetering balance of the level of risk under which the system is subjected, the level of trust placed on the individuals with access to the system, management's perspective or requirement for monitoring of system functions and data manipulation, as well as the time allocated for performing or monitoring the audits. The more auditing features turned on the more voluminous the audit reports and the more time required to adequately review and decipher the alerts, warning, and information provided.

To view the current Audit setting: Click Start, Programs, Administrator Tools (Common), User Manager for Domains. When the User Manager Screen Opens, Click on the Policies Pull Down Menu and select Audit Policy.

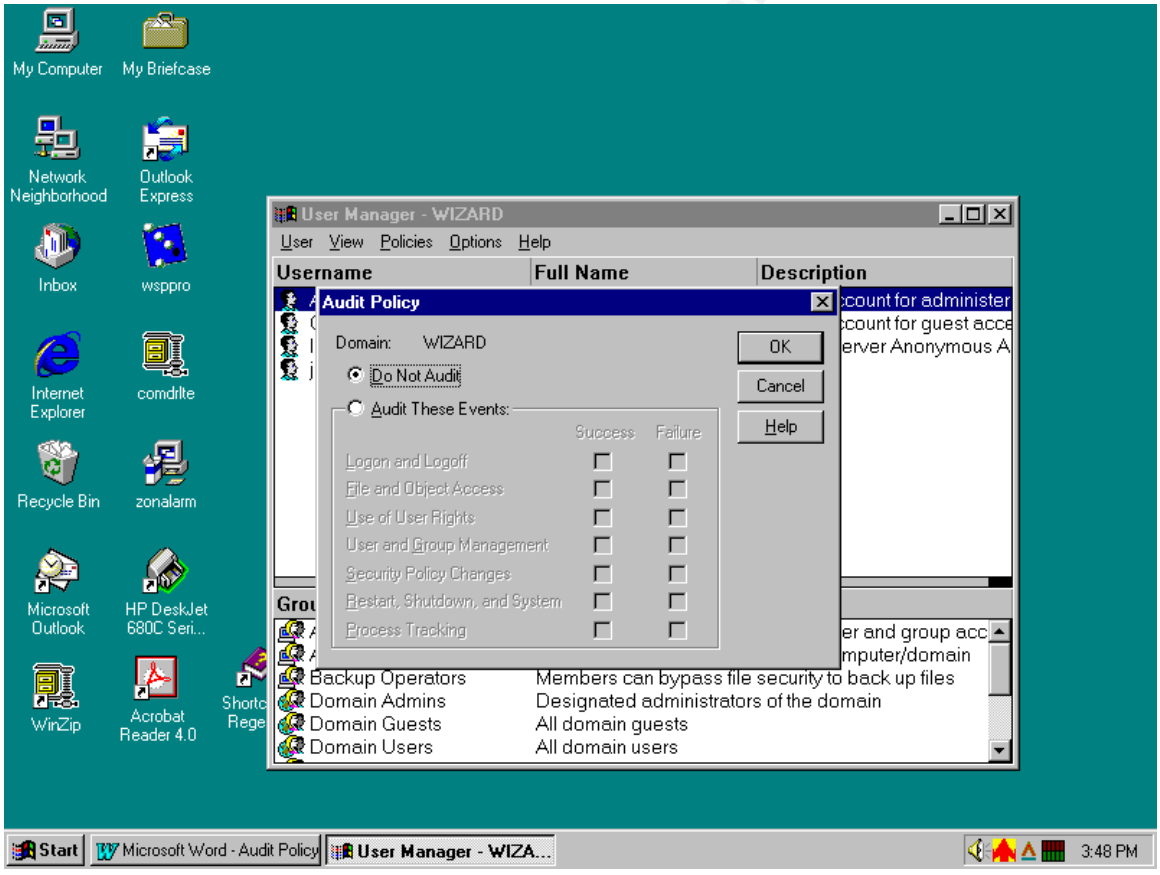


Figure 8.

Figure 8 displays the default setting, as shown. "Do Not Audit" is selected and all of the audit events have been grayed out.

The DON Recommended Audit Events

Logon and Logoff	Success and Failure
File and Object Access	Failure
Use of User Rights	Failure
User and Group Management	Failure
Security Policy Changes	Success and Failure
Restart, Shutdown, and System	Success and Failure

Table 2

To turn Auditing on, Select "Audit These Events", the individual Events will then be enabled. Figure 9 displays the implementation of Audit events recommended by DON as defined in Table 2.

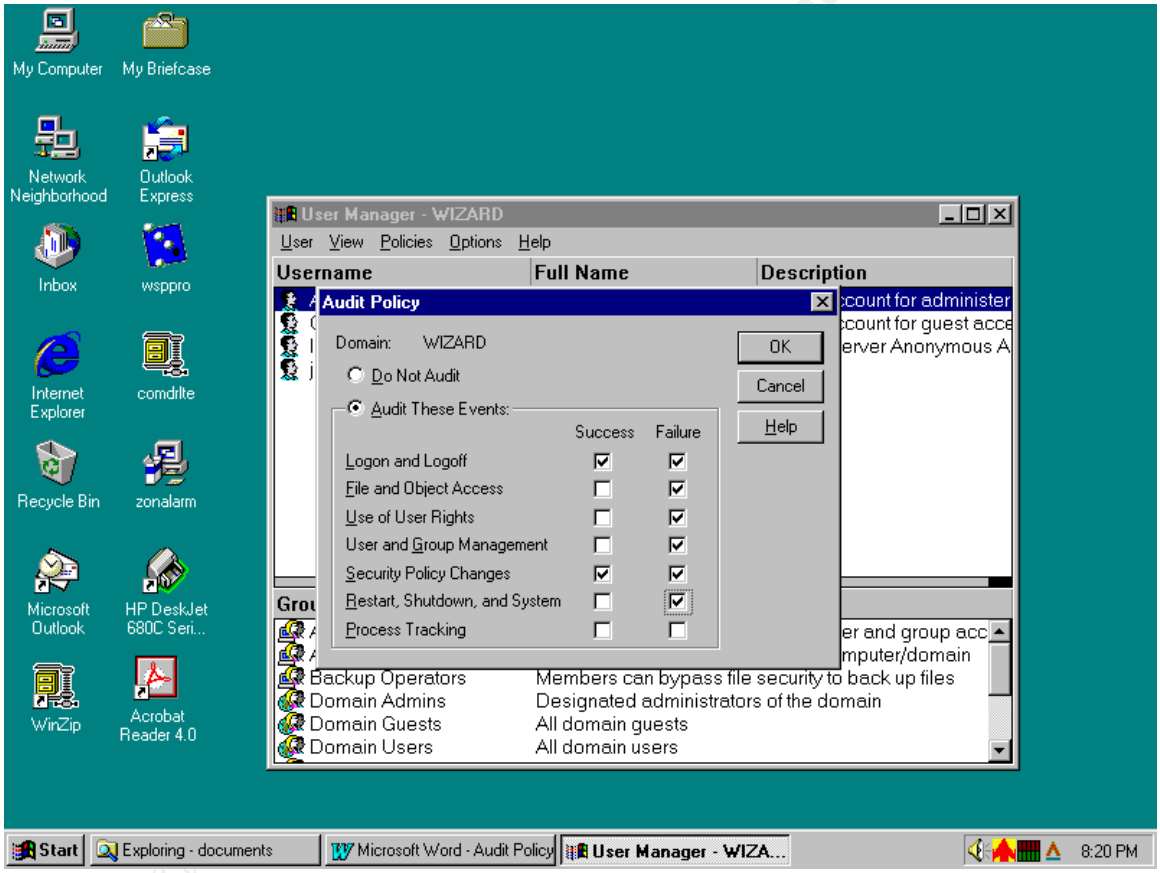


Figure 9.

The Audit log files must also be configured. WinNT has three audit logs, System Log, Security Log, and Application Log. The maximum log size and retention period must be set for each of the three Audit log files. These setting are implemented in the Event Viewer. Click Start, Programs, Administrative Tools (Common), Event Viewer. Select Log in the Event Viewer as shown in Figure 10.

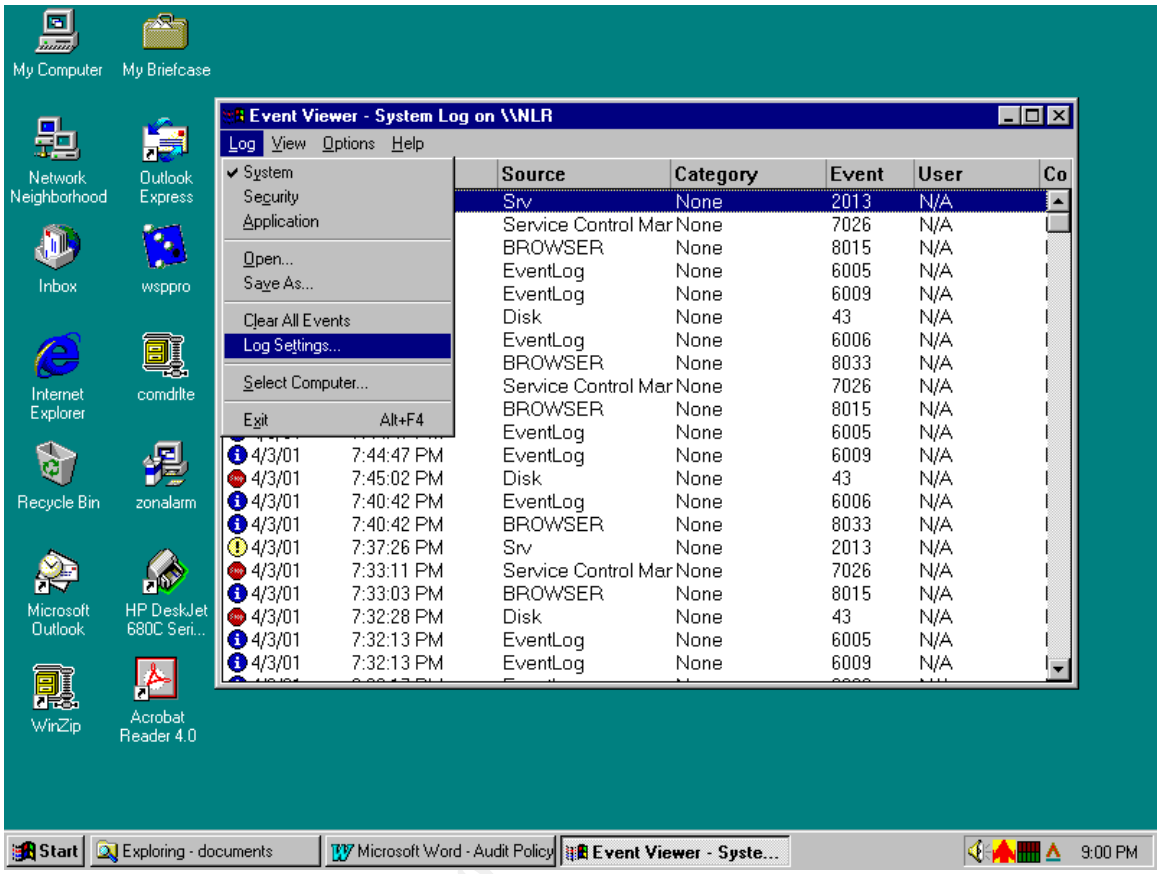


Figure 10.

The default settings are for 512K of disk space and to "Overwrite Events older than 7 days." Figure 11 below displays the default settings.

DON recommendations establish the file size for all three logs to 4194K. This setting will depend on the size of the network, server, number of users, and the frequency of logged events.

The Event Log Wrapping is a critical setting. NT will crash the server if the log runs out of space. Setting it for "Do not Overwrite Events" (Clear Log Manually) or Overwrite in 7 days (the default) could cause system availability to be interrupted if the administrators are not diligent in clearing the log or if an incident occurs where the log is filled quickly and unexpectedly. These options are not recommended.

"Overwrite Events Older than X days" normally will provide the server with the greatest flexibility in monitoring the Event Logs and capturing the logged events for historical reference. The log fill rate will depend on the activity on the server. Using this setting will required an in-depth knowledge of the specific server and the traffic activity as well as requiring dedicated monitoring.

"Overwrite as Needed" could provide an attacker an opportune environment to force the log to overwrite to cover their tracks after an intrusion as discussed by Otis Brig in his work "Track 5: Windows Security"[4]. Given that threat DOD recommendation remains "Overwrite as needed." This option provides the greatest level of assurance the NT operations will not be interrupted due to lack of space in the log files. An aggressive archive policy will help mitigate the risk of data lost due to attacker manipulation to an acceptable level.

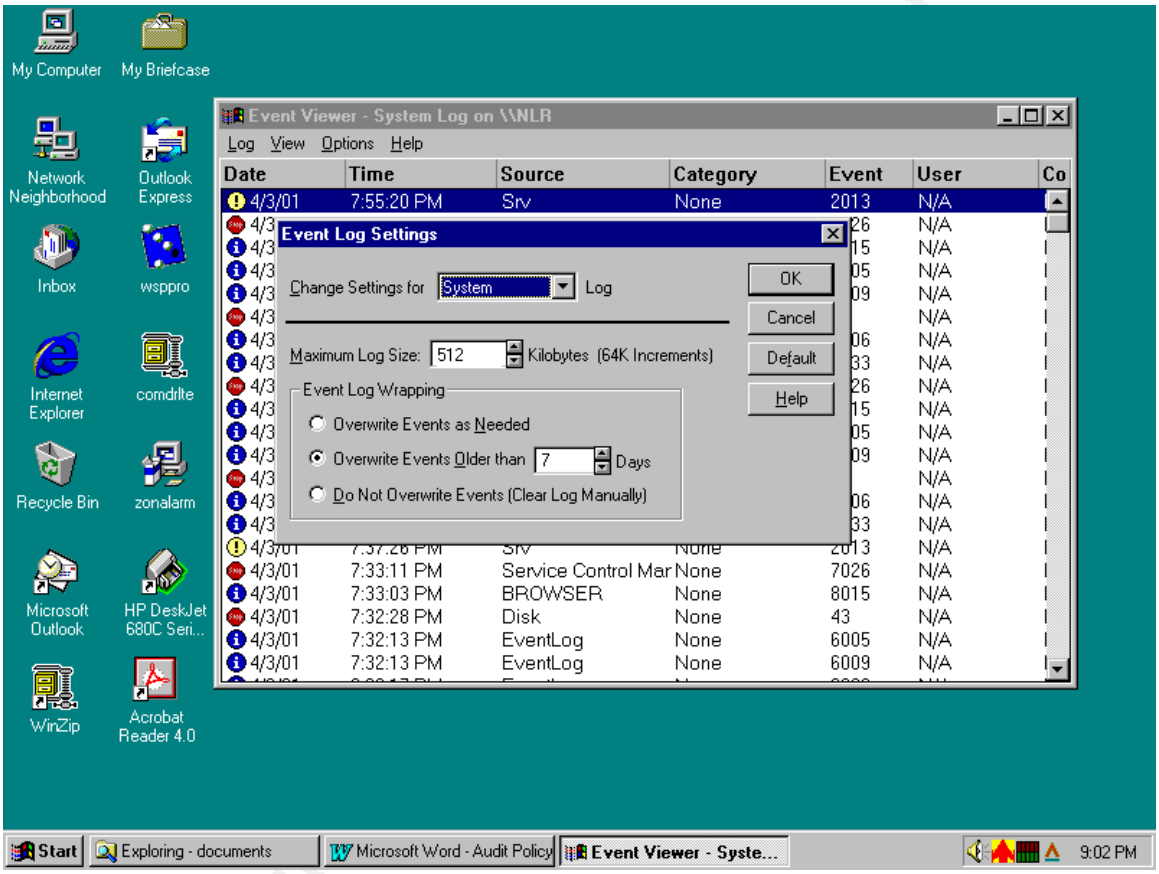


Figure 11.

The Events are viewed in the Event Viewer, Select the Log file to view, from the Log Pull Down Menu. Events will be displayed with newest entry first. No filters are turned on as a default, so all events will be displayed. Filtering can be turned on by selecting the Options Pull Down Menu as displayed below in Figure 12. Date Ranges for viewing the events can be set as well as determining which events should be reviewed.

Items available on the Filter menu: “Source” is the software that logged the event. “User” will display the exact Username field that caused the logged event. The “Category” refers to the setting this Audit Procedure defined under the Accounts section of this paper. Logon, Logoff, etc. “Computer” displays the

computer name or host name. “Event” will display an event number. Event numbers can be researched on the http:\\support\microsoft.com web site for additional information on what caused the event. There are five types of events: Information Events, Warning, Error Success Audit and Failure Audit. “Information” is used by applications to log the successful completion of services or program runs. “Warning” denotes items that aren’t really troublesome at the time, but may cause a problem later. “Error” denotes a major problem that should be researched and corrected immediately. “Success Audit” and “Failure Audit” denotes security-access events. The category would specify which event was logged.

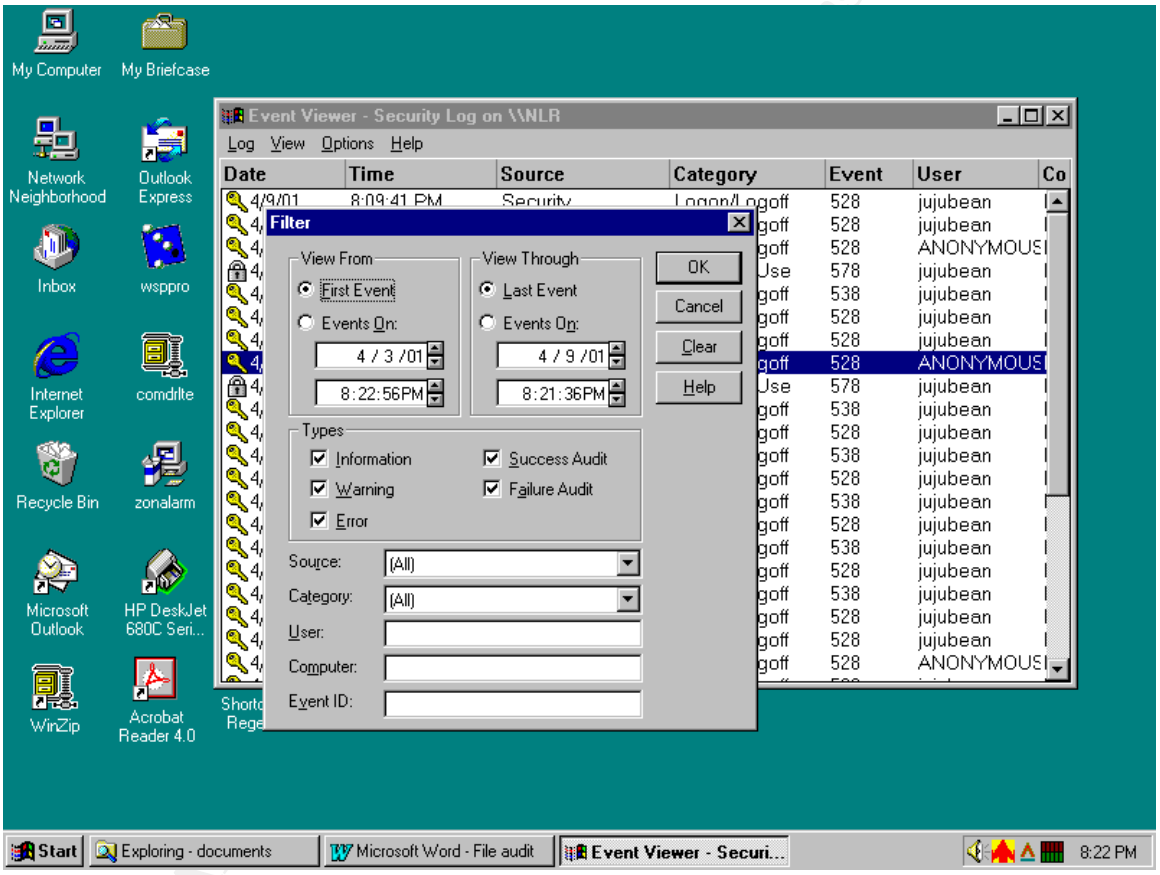


Figure 12.

Figure 13 below display an Event Detail. This event was logged as a Success Audit, from computer name NLR, the event was Logon/Logoff.

The Logon Type will denote the method used for system access. Logon Type 3 as listed in Figure 13 is a network logon. Additional Logon Types:

Logon Type 2	Interactive logon from the system console,
Logon Type 4	System access initiated from a batch process,
Logon Type 5	System access started by a service,

Logon Type 6 System access via a Proxy,
Logon Type 7 Access from a locked system console.

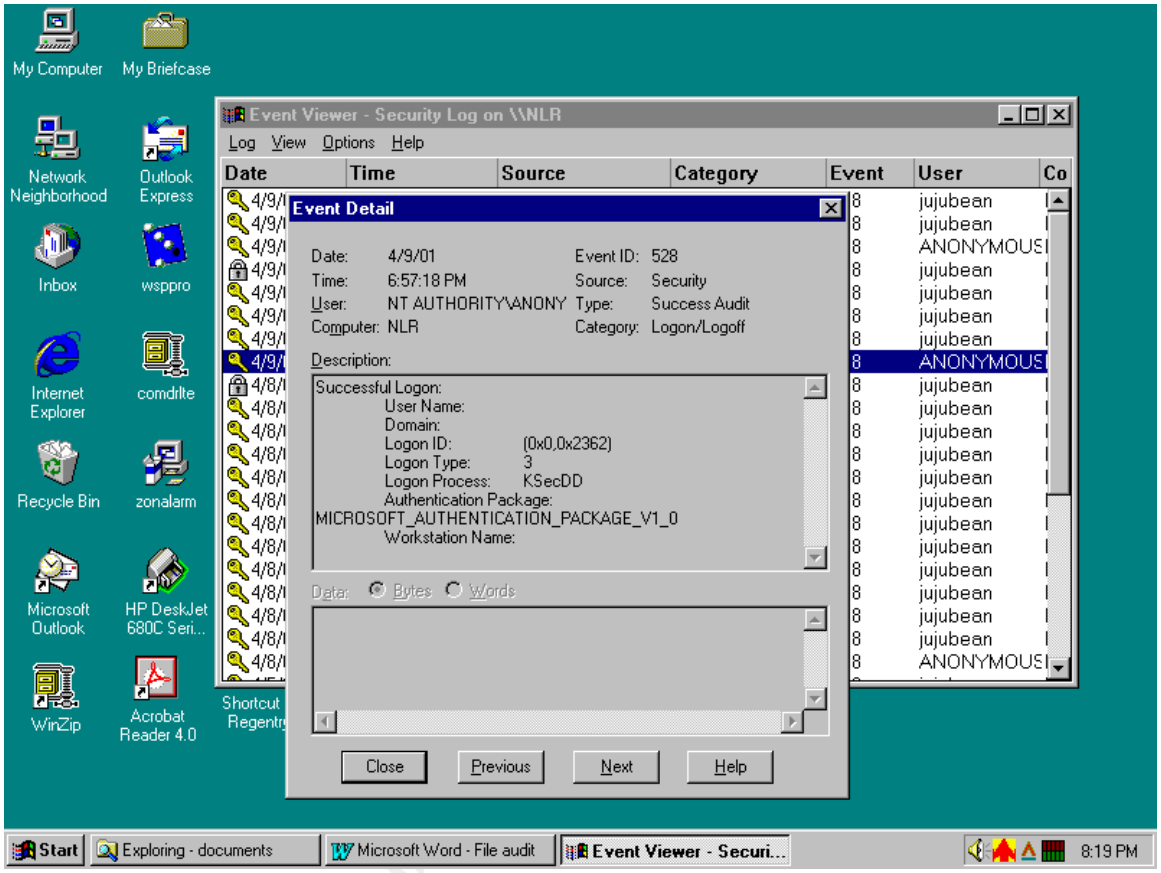


Figure 13.

Archive Planning:

An Archive Plan must be determined and implemented to provide historical records for Audit Events. DON recommends all Audit Logs be maintained for one year. These historical records can provide usage statistics, troubleshooting chain-of-events and Forensic evidence in case the system is attacked. To be used as forensic evidence the files must be maintained regularly, for administrative purposes as well as historical reference, and be stored in a pristine manner to prevent tampering or unauthorized modification.

Events can be archived in either .EVT format or .TXT format. Log files archived as .EVT files can later be reviewed using the Event Viewer. ".TXT" files can be saved in delimited format for use in a spreadsheet or database. The sort in effect when the event log is archived will be retained. Events archives included all events and is not limited to those shown by the filter parameters set at the time.

Note: If reviewing the log files archives in Event Viewer ensure that the Log type is set to match the Log file being viewed. If the Log type archived is the Security Log but the Event Viewer is set on Application Log when the archive is being reviewed, the data will seem distorted.

Monitoring Audit Logs and System conditions is a time consuming and complex task. Several utilities are provided with Stock WinNT and with NT Resource Kit to assist the Administrator in capturing and reviewing the Audit logs. Tables 3 and 4 provide a partial list to get started, the many commands have multiple parameters to obtain system statistics. Review the commands and their syntax in Windows NT Help and in command line help.

Stock WinNT Utilities

UTILITY	SYNTAX	DESCRIPTION
net.exe	NET HELP command -or- NET command /HELP	used to collect user and group info, many different qualifiers can be used, server, computername, etc.
sysdiff.inf	sysdiff /snap	to create initial baseline
sysdiff.inf	sysdiff /diff baseline.img diff.img	identify differences in the two files
sysdiff.ini	sysdif /dump	output to human readable format
netstat	netstat –a >listen.txt	snapshot of ports/processes open ATT
netstat	netstat –a | more	prints to screen hit enter to view next screen
netstat	netstat –n	Displays addresses and port numbers
netstat	netstat –p *protocol*	Shows connections for the specified protocol
ntlast	ntlast	used in Event Viewer to filter alerts
net start	net start	shows services on local system only
regdmp.exe	regdmp –m \\ SERVER > regfile.txt	create and ASCII vs. of registry
xcacls.exe	xcacls c:\winnt\system32\hackme.exe	hackme=a file that you do not think belongs queries a single file for the access level of multiple users
perms.exe	perms domain\user c:\winnt*.exe	query multiple files for the access level of a single user
dir	dir | more	used to check size and date/time as to their creation or last access time

Table 3.

NT Resource Kit Utilities

UTILITY	SYNTAX	DESCRIPTION
dumpel.exe	dumpel –l security –f logon.txt –s server –c	-l the log to dump –f name of export file –s name of remote system to query. Used to dump the log to an ASCII text file. Can also filter the events exported based on source service or event ID number.
Netsvc.exe	netsvc.exe //server /list >service.txt	documents services and drivers running
adduser.exe	adduser \\server /d user-grp.txt	
findgrp.exe	Findgrp accountname	show all local and domain groups for a user
global.exe	Global group_name domain_name | \\server	show all members of a specific domain group

local.exe	Local administrator \\servername	show all members of a specific local group
Auditpol.exe	Auditpol \\servername	Displays the active audit policy set on the server
Tlist.exe	Tlist	List the tasks and process id (PID) currently running on the server

Table 4.

The system administrator should determine an effective schedule for running commands, including those above, to obtain a sound baseline of the system and to create historical records. The auditcat.hlp provides additional information to assist in the review and understand event logs alerts

Note: The Audit Logs are located in \\server\winnt\system32\config directory.

The following batch file is provide to assist system administrators in the task of running statistical commands and creating historical records. This file is submitted as a template, which can be modified to meet each system's specific needs.

---

audit.cmd

```
@echo off
rem  Audit Batch by Nancy Roberts/SANS roberts005   12 Apr 01
rem
rem  The batch file contains stock and NT Resource Kit commands to
rem  assist the system administrator in conducting auditing and
rem  monitoring results.
Rem
rem  dumpel will dump the Event log files in a selected output file
rem
dumpel –l security –f d:\logs\security.txt –s servername –t
dumpel –l application –f d:\logs\appl.txt –s servername –t
dumpel –l system –f d:\logs\system.txt –s servername –t
rem
rem  tlist list the tasks and process id (PID) that are running on a
rem  Windows NT machine, good for a local server only, must use PULIST
rem  if you are trying to run on a remote server.  Provided by Back Office
rem  Resource Kit
tlist > tlist.txt
rem
rem  net share will display information about all shares on a server
net share > netshare.txt
```

```
rem
rem  net start will display services started on the server
net start > netstart.txt
rem
rem  netstat will display the process and protocols running on local server
netstat –a > netstat.txt
rem
rem  netsvc will display the services running on the server
netsvc \\servername /list > netsvc.txt
rem
rem  auditpol will show the active audit policies set on the server
auditpol \\servername > auditpol.txt
rem
rem  local will display the members of the administrator group on the server
local administrator \\servername > local.txt
rem
rem  logevent will add “Audit program successful” in the event log.
Logevent “Audit program successful”
rem
rem  logtime creates log entry for the time the audit batch file runs
logtime “completed audit batch”
rem
rem  audit.kix is a kixtart batch file that will zip the txt and log files created in the
rem  audit.cmd and then move the zip file to a new directory named after the
date
rem  the program was run,
kix32 audit.kix
```

---

audit.kix [6]

```
$DATE=”@YEAR@MONTH@MDAYNO”
md “\\pathname to directory\LOGS\$DATE”
shell “zip.bat”
COPY “dailylog.zip” “\\pathname to directory\LOGS\$DATE\”
DEL “dailylog.zip”
```

---

zip.bat

```
pkzip –a –ex –m dailylog.zip *.txt
pkzip –a –ex –m dailylog.zip *.log
```

---

md5 dailylog.zip dailylog.crc [7], [8]

---

check.bat [9]

```
@echo off
For /F "Tokens=1" %%i in ('type %1.crc') do set CRC=%%i
md5 -c%CRC% %1.zip
If errorlevel 1 goto 1
:0
echo Unchanged
goto end
:1
echo Changed
:end
```

****

The system administrator must modify the above program files to reflect the name of their individual server and to define the pathname to a restricted access folder for storage of the files on a daily basis.

The audit.cmd file as written will capture duplicate information in the security.evt, application.evt and system.evt log files due to the log wrapping set to "Overwrite as Needed". This is viewed as an safety measure. Program driven clearing of the event logs is not recommended. To avoid clearing logs prior to verification of successful archiving, manual clearing on a weekly basis is recommended.

The KIXTART 95 program is available in public domain and was originally shipped with Windows NT (http://www.comptrends.com) and greatly enhances the capability of using script files for WinNT and Windows 2000.

Pkzip was used instead of WINZIP based on its flexibility in command line use. WINZIP will open and operate on the zip files created with the zip.bat above without any difficulty, users do not need to change to Pkzip.

The MD5 utility command line will produce a 32 character digital signature. This can be used to validate the dailylog.zip file has not been modified since it was written. This utility must be run from the directed where the specific dailylog.zip file is resident and the system administrator must ensure that the MD5 hash digital signature stays in the directory as well. A MD5 logbook can also be used to ensure accuracy. If a logbook is used, it should be stored in a safe, or other secure location.

The next step in creating historical records is to write the directory, dailylog.zip and dailylog.crc to a CD-ROM, preferably on a weekly basis.

The check.bat can be used at any time to compare the original .crc files and the .crc of the file at that time. The check.bat will run a new MD5 hash and then display a “Changed” or Unchanged” finding to the screen.

To further automate the process the system administrator should issue the AT command:

At \\servername 0500 /EVERY:M,T,W,Th,F audit.cmd

The Task Scheduler “AT” command will allow the system administrator to issue the batch file to the schedule to run at the same time every day without daily intervention. Only issue the AT command once to run the audit.cmd batch file. (The AT command/Task Scheduler and will issue the command to run once for every time that it is entered in to the system.)

A zip file is submitted with this practical that contains the program files, and .dll files required to successfully execute the above programs. The MD5 Hash is public domain and source and executables are included in the zipped program file.

File/Folder Protection:

The Audit log folder should be restricted to audit personnel as a subset of system administrators, to limit the possibility of unauthorized modification of the logs. A detailed explanation of setting file/folder permissions is deferred to Michael J. Moore's extensive guide to Auditing a Folder Object in his work "Issues with Auditing Windows NT 4.0 Server.(*) To modify permissions on a specific folder or files, right click on Start and open Explorer, navigate to the desired folder or file, highlight and right click. Select Properties to display the property page. Select the Security tab and click on Permissions. This will display a window with the current permissions. The default permissions is "Everyone" "Full Control". Click on Add to display the system and local groups and select the Audit group if one is available if not, select the individuals that will require access to the Log Folder. Include the Task Scheduler. Figure 14, below shows the permission modification for the Log Directory. File/Folder permissions can be used for other areas where the administrator needs to limit access.

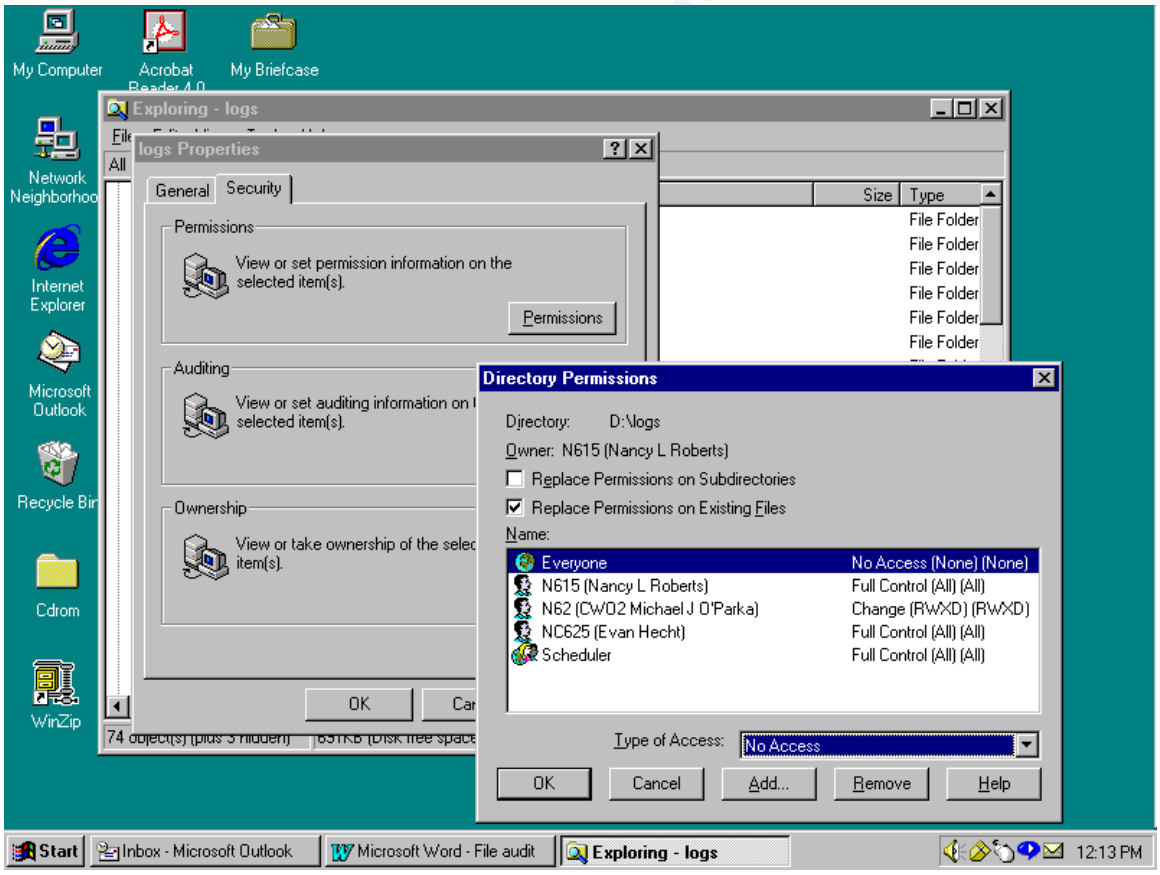


Figure 14.

Registry:

The Registry is a critical element in NT/2000 configuration and contains the rule set that Auditing will use to determine authorized and unauthorized events. Appendix A contains a listing of the "Navy flavor or NSA PDC (SP6a)" .inf template for use with Security Configuration Manager (SCM). A review follows of the Registry for those less familiar with its intricacies.

Since the Registry can be administered remotely and contains hardware and user specific configuration information special care must be taken to protect it from unauthorized modification or destruction. The MCSE's at New Riders take it even further by recommending, "… Remove REGEDT32.EXE from every WinNT workstation that no administrator will use. Administrators can edit remote registries without leaving their own workstations, so making REGEDT32.EXE available locally at every workstation isn't necessary." (10)

The first level of protection that Microsoft provides is by reducing the visibility of the Registry. The Registry Editor file (REGEDT32.EXE) is not listed in the Menu items for Program files, nor is an Icon installed on the Desktop under either user or Administrator accounts. Microsoft provides a user-friendly interface for the registry by implementing most basic changes to a system configuration through GUI interfaces such as Control Panel Icons. The System Policy Editor takes up where Control Panel stops providing another layer of GUI interface protection. By providing the GUI interfaces, Microsoft limits the requirement for manual changes to the Registry to only those that can not be accomplish through protected front-end programs.

The Registry is grouped in Hives, so named by Microsoft for the busy functionality and the myriad of tunnels and paths involved. The Hives are stored in the winnt\system32\config and the winnt\profiles\username directories. There are two pre-defined keys in the Registry that structure the rest of the registry elements. HKEY_LOCAL_MACHINE (HKLM-list computer specific configurations) and HKEY_USERS (HKU-list user specific configurations). Three of the remainder of the Root keys is symbolic keys that link to the HKLM and HKU keys. HKEY_CLASSES_ROOT contains OLE and file association information much the same as the Win.ini file of earlier versions of Windows and is provided to maintain compatibility with Windows 3.x programs It is a duplicate of the information stored in the HKEY_LOCAL _MACHINE\SOFTWARE\Classes key. The HKEY_CURRENT_CONFIG links to the HKEY_LOCAL_MACHINE key and provides hardware profiles for the current NT Load. HKEY_CURRENT_USER links to the HKEY_USERS key and provides profiles for the currently logged on user. (11)

The remaining Root Keys are Virtual Links, HKEY_DYN_DATA is used for Windows 9x systems and HKEY_PERFORMANCE_DATA is used for NT/2000 systems performance data. Figure 15, shows the Hives as viewed from

REGEDT32.EXE.

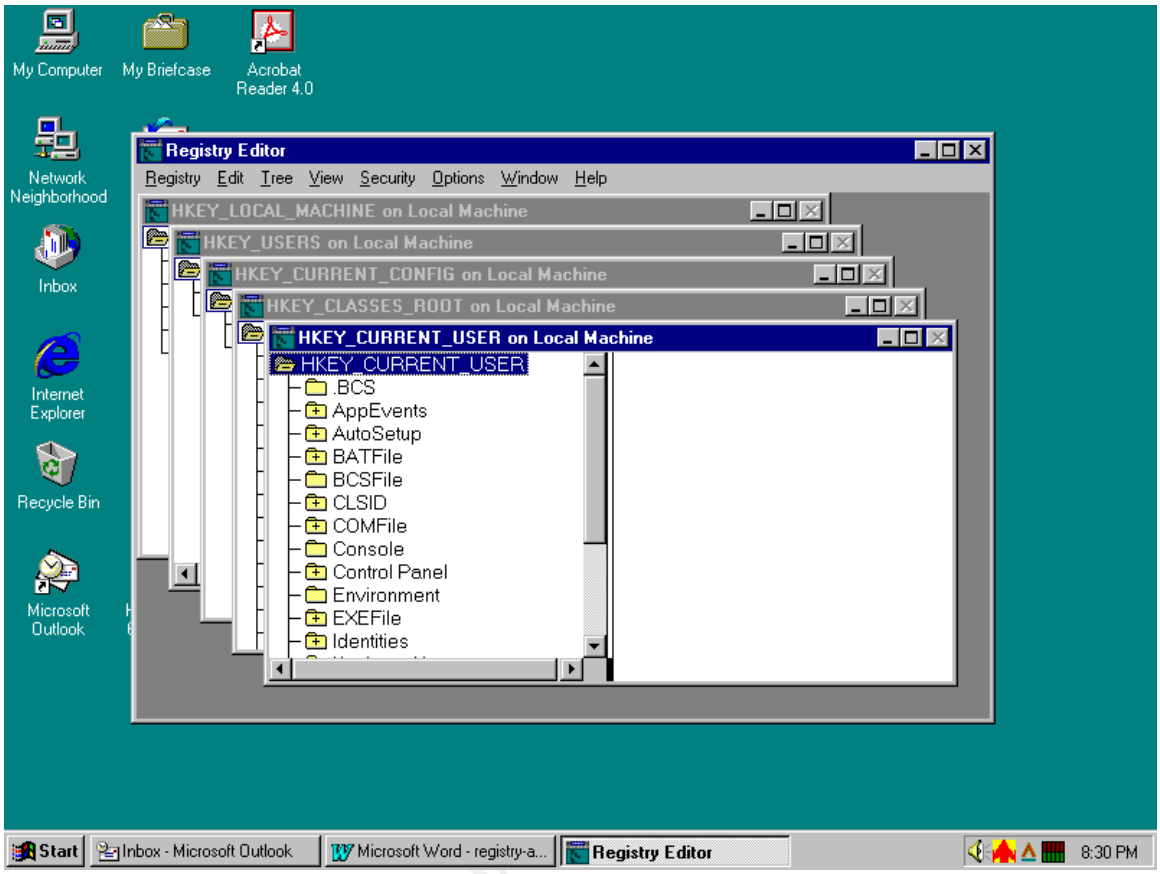


Figure 15.

There are two files associated with each Hive and named after the hive, one without an extension and one with the (hive name).log extension.

Prior to modifying the Registry, the Administrator should make sure that adequate backups have been prepared. The log files are in constant transition and are used to annotate a change to the Hive prior to its successful implementation. If the modification does not complete successfully, this provides a way for the NT Loader to revert back to the previous load (LASTKNOWNGOOD). Registry .log files do not require backup.

The System and Software files are usually open during normal backup procedures so need to be specifically backed up using the RDISK command. RDISK will backup System and Software in the repair disk directory, however the RDISK /S must be used to backup the SAM and Security files. After backing up the files each Sub-tree should be printed to aid in making changes or verifying settings as shown in Figure 16.

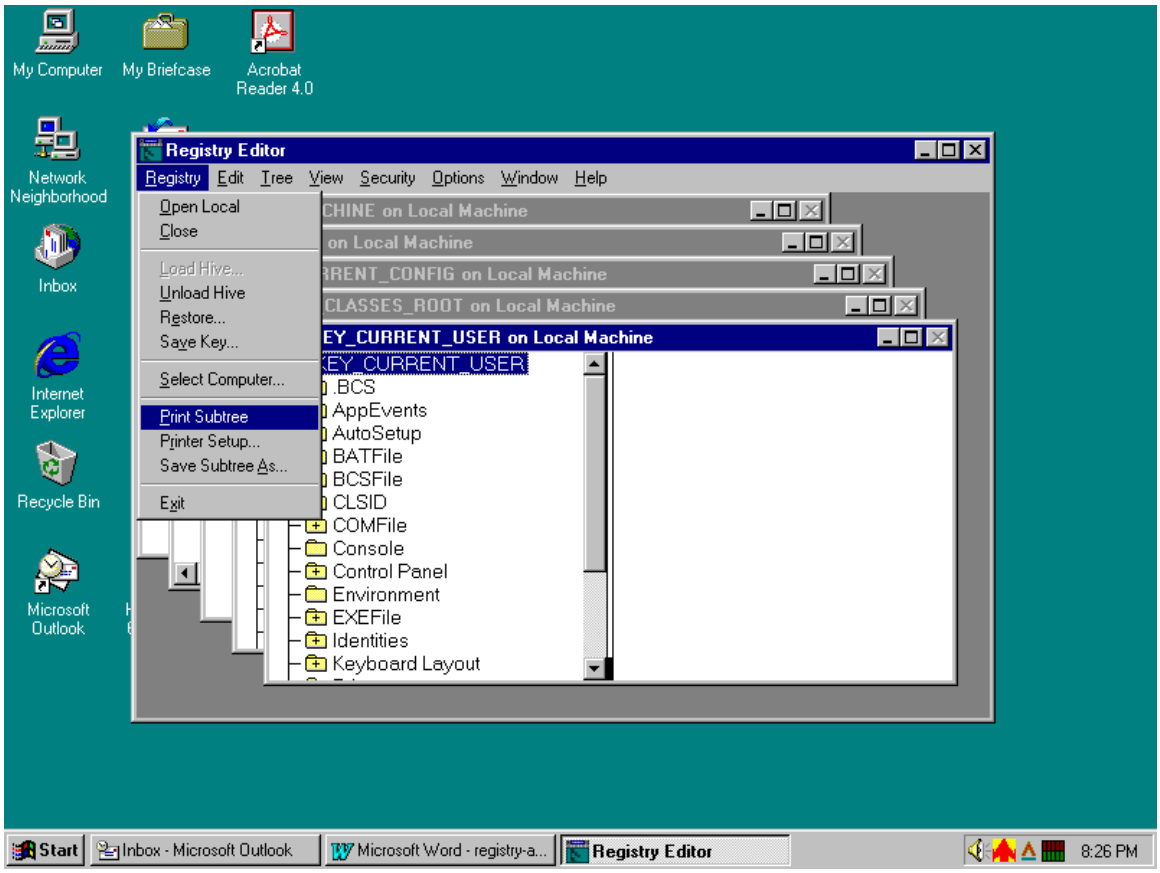


Figure 16.

Understanding the Registry is truly a fine art. For those still struggling to gain the secret to Microsoft's Registry, Regentry.HLP is available from the NT Resource CD or for free from ftp.microsoft.com.

The default NT installation does not turn auditing on for Registry files such as the SAM file. Auditing Registry Key is not required but can be turned on by highlighting the desired key, Select Audting, (Figure 17). The SAM audit menu is shown in Figure 18. Select "Audit Permissions on Existing Subkeys" and then Adding the domain, and user or group accounts to be monitored.

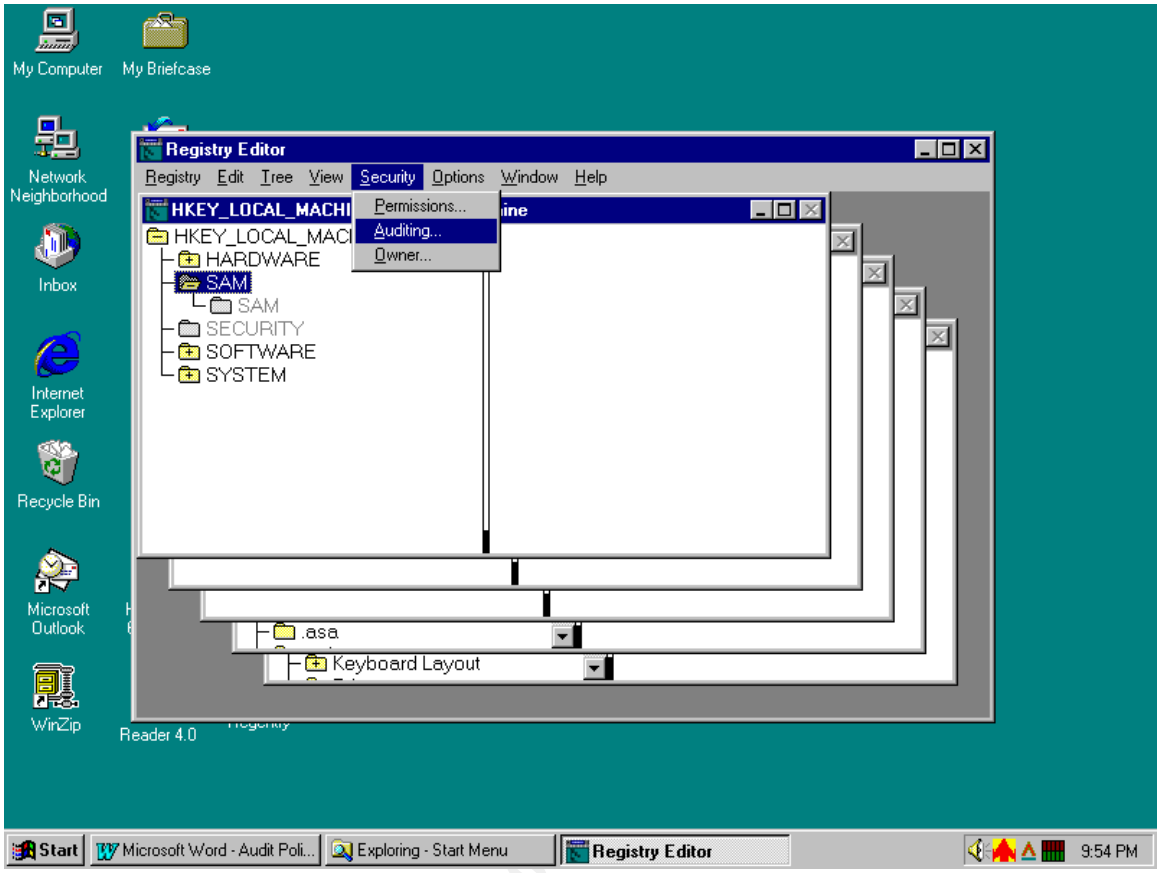


Figure 17.

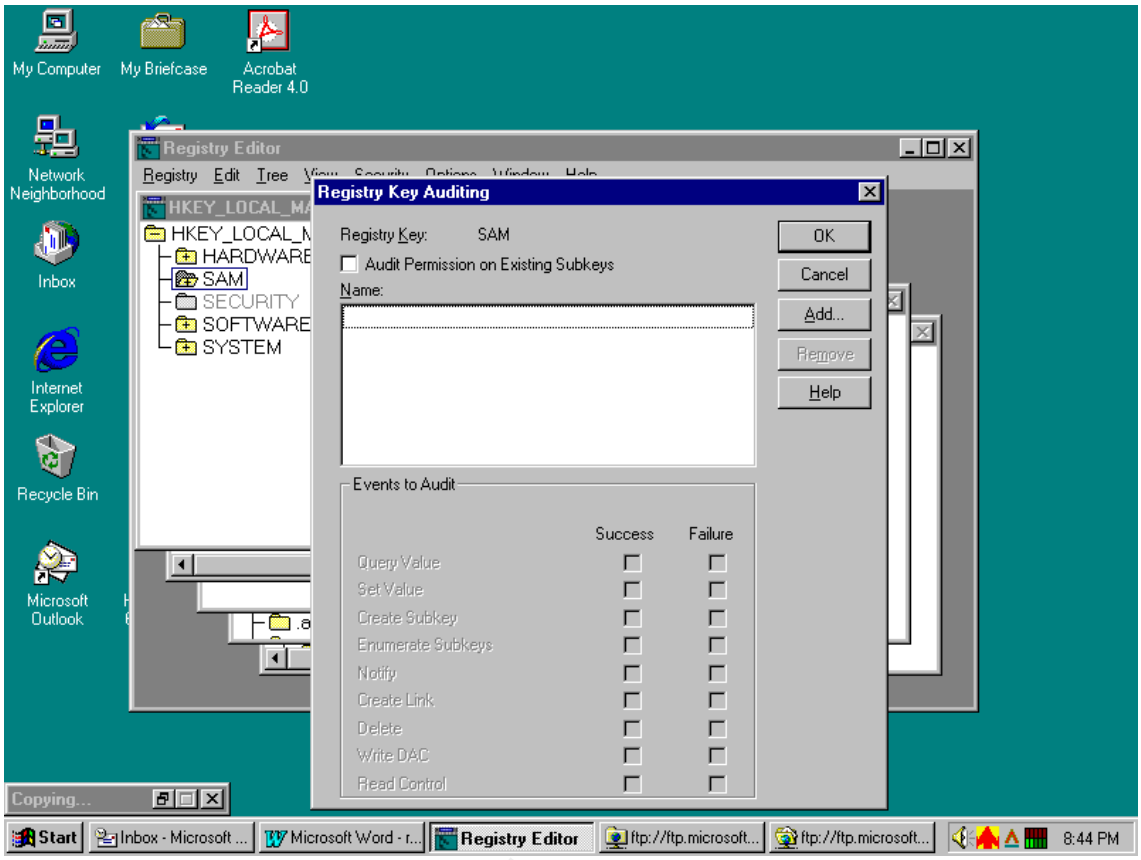


Figure 18.

The Security Configuration Manager (SCM) provides another GUI interface for implementing WinNT configuration setting. (SCM can also be used in a command line mode.) SCM plug-in was not provided with the original delivery of WinNT 4.0 but can be downloaded from Microsoft at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm.

Lisa Yeo [12] outlined the use of SCM for configuration management specifically for Internet Information Server (IIS4) but SCM can be used to implement a variety of security requirements through the use of pre-configured templates or by implementing a custom developed template. The system administrator can consolidate all the settings required into a custom template, ensuring standardization across multiple platforms. Appendix A provides a copy of the Navy flavor of NSA PDS (for SP6a) .inf file that can be implemented through Security Configuration Manager.

Footnotes

(1) Moore, Michael J., “Issues with Auditing Windows NT 4.0 Server”, http://www.sans.org/giactc/gcnt/Michael_Moore.doc, Dec 2000.

(2) U.S. Navy ”Trusted Security Evaluation Criteria (TCSEC) “ Slide presentation, Information Systems Security Manager Course, Aug 2000, (pg. 34).

(3) Heckendorn, Sherri. SANS Practical, not named, http://www.sans.org/giactc/gcnt/Sherri_Hechendorn.doc, (pg. 15).

(4) Hutchinson, George. “Securing Windows NT 4.0 based Networks”, http://www.sans.org/giactc/gcnt/George_Hutchinson.doc, (pg. 13).

(5) Otis, Brig. SANS Practical, Track 5: Windows Security Monterey, http://www.sans.org/giactc/gcnt/Brig_Otis.doc, 2000. (pg. 19).

(6) Hecht, Evan. Kixtart utility, audit.bat, April 11, 2001.

(7) Rivest, Ron. MD5 algorithm, http://www.fourmilab.ch/md5/. Public Domain.

(8) Plumb, Colin. MD5 C language utility, http://www.fourmilab.ch/md5/. Public Domain.

(9) Hecht, Evan. Windows utility, check.bat, April 13. 2001.

(10) Casad,et al. MCSE Windows NT Server and Workstation 4 Study Guide. New Riders Publishing. 1996. (pg. 457).

(11) Casad,et al. MCSE Windows NT Server and Workstation 4 Study Guide. New Riders Publishing. 1996. (pg. 459).

(12) Yeo, Lisa. “Configuring and Auditing Windows NT with Security Configuration Manager”, http://www.sans.org/giactc/gcnt/Yeo_Lisa.doc, Sept 2000.

References

Carrington, Richard. "Scripting with NT Resource Kit, part 1: The essentials. TechProGuide. Apr 13, 2000. TechRepublic, Inc. 2001.

Carrington, Richard. "Scripting with NT Resource Kit, part 2: More Simple Commands. TechProGuide. Apr 20, 2000. TechRepublic, Inc. 2001.

Carrington, Richard. "Scripting with NT Resource Kit, part 3: Commands for local and remote servers. TechProGuide. May 8, 2000. TechRepublic, Inc. 2001.

Casad,et al. MCSE Windows NT Server and Workstation 4 Study Guide. New Riders Publishing. 1996.

Heckendorn, Sherri. SANS Practical. http://www.sans.org/giactc/gcnt/Sherri_Hechendorn.doc.

Hutchinson, George. "Securing Windows NT 4.0 based Networks", http://www.sans.org/giactc/gcnt/George_Hutchinson.doc, pg. 13-15.

Moore, Michael J. "Issues with Auditing Windows NT 4.0 Server". http://www.sans.org/giactc/gcnt/Michael_Moore.doc, Dec 2000.

Otis, Brig. SANS Practical, Track 5: Windows Security Monterey. http://www.sans.org/giactc/gcnt/Brig_Otis.doc, 2000, pg. 19-23.

Microsoft Windows NT Server Resource Guide. Microsoft Press. 1996.

SANS Institute. *"Windows NT Security Step by Step, A survival guide for Windows NT Security."* Vs. 2.15. 30 July,1999.

"Security Configuration Editor". Microsoft Corporation, 1998. ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm/readme.txt.

Tomlinson, Paula."Understanding NT." Windows Developer's Journal. Vol. 12, #1. Jan 2000. pg 54.

United States. Department of Defense. DoD Directive 5200.28, *Security Requirements for Automated Information Systems (AISs)*

United States. Department of Defense. DoD Directive 5200.1R, *DoD Information Security Program*.

United States. Department of Defense. DoD 5200.28-STD, *Trusted Computer*

System Evaluation Criteria, Orange Book, Dec 26, 1985

United States. Department of Defense. DISA Instruction (DISAI) 630-230-19, *Security Requirements for Automated Information Systems (AIS)*

United States. Office of Management Bureau. OMB Circular No. A-130, *Management of Federal Information Resources*

United States. Department of Navy. Chief of Naval Operations. OPNAV Instruction 5239.1B, *Navy Information Assurance Program*

United States. Department of Navy. Commander Space Warfare Systems Center. SPAWARSYSCEN PMW161, *Secure Windows NT Installation and Configuration Guide,* May 1999.

United States. Department of Navy. Commander Space Warfare Systems Center. SPAWARSYSCEN PMW161, *Secure Windows NT Installation and Configuration Guide,* vs. 1.5, Sep 27, 2000.

United States. Department of Navy. Commander Navy, Education and Training. ”Trusted Security Evaluation Criteria (TCSEC) “ Slide presentation, Information Systems Security Manager Course, Aug 2000.

Walker, John. MD5: Command Line Message Digest Utility. http://www.fourmilab.ch/md5/. Jan 6, 2001.

Windows NT 4.0, SP6A, On-line Help Command.

Appendix A-Navy Flavor of NSA PDC (for SP6a)

```
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 180
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 5
LockoutBadCount = 5
ResetLockoutCount = 30
LockoutDuration = 30
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 1

[System Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1


[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 0
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 0
CrashOnAuditFull = 0


[Version]
signature="$CHICAGO$"


[Group Membership]
```

[Registry Values]
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects=4,0
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnablePlainTextPassword=4,0
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown=4,1
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\AddPrintDrivers=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ShutdownWithoutLogon=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption=1,United States Department of Defense Warning Statement
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText=1,This is a Department of Defense computer system. This computer system,including all related equipment,networks and network devices (specifically including Internet access),are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes,including to ensure that their use is authorized,for management of the system,to facilitate protection against unauthorized access,and to verify security procedures,survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of the system. During monitoring,information may be examined,recorded,copied and used for authorized purposes. All information,including personal information,placed on or sent over this system may be monitored. Use of this DoD computer system,authorized or unauthorized,constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative,criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\DontDisplayLastUserName=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,15
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1

MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,31
MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl=4,1

[Registry Keys]
"MACHINE\SOFTWARE\ODBC",0,"D:(A;;CCDCLCSWRPRC;;;AU)"
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"
"CLASSES_ROOT\.hlp",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"
"MACHINE\SOFTWARE",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0003001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Protected Storage System Provider",1,""
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility",2,"D:P(A;CI;0xc0000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;CO)(A;CI;0x10000000;;;SY)"
"MACHINE\SOFTWARE\Program Groups",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"
"MACHINE\SOFTWARE\Secure",2,"D:P(A;CI;0x10000000;;;CO)(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
"USERS\.DEFAULT\SOFTWARE\Microsoft\Protected Storage System Provider",1,""
"MACHINE\SYSTEM\CurrentControlSet\Services\UPS",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"
"MACHINE\SYSTEM\CurrentControlSet\Services\Schedule",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"
"MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"
"CLASSES_ROOT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x0002001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"
"CLASSES_ROOT\helpfile",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
"MACHINE\SOFTWARE\Classes",1,""
"MACHINE\SOFTWARE\Microsoft\Cryptography",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)(A;CI;0x80000000;;;AU)"
"MACHINE\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Ole",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;CO)(A;CI;0x10000000;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Rpc",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"

"MACHINE\SOFTWARE\Microsoft\Secure",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x
00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Windows",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;
0x0002001f;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce",2,"D:P(A
;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x10000000;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(
A;CI;0x000f003f;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AeDebug",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;A
U)(A;CI;0x000f003f;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font
Drivers",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;
SY)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\FontMapper",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;
;;AU)(A;CI;0x000f003f;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution
Options",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI;0x1000000
0;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\IniFileMapping",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000
000;;;DA)(A;CI;0x10000000;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Perflib",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(
A;CI;0x000f003f;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;
DA)(A;CI;0x10000000;;;SY)"
"USERS\.DEFAULT",2,"D:P(A;CI;0x80000000;;;AU)(A;CI;0x10000000;;;DA)(A;CI
;0x10000000;;;SY)"
"USERS\.DEFAULT\SOFTWARE\Microsoft\NetDDE",2,"D:P(A;CI;0x10000000;;;
DA)(A;CI;0x10000000;;;SY)"
"USERS\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies",2
,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;CO)(A;CI;
0x000f003f;;;SY)"
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for
NT",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x000f003f;;;CO)(A;CI;0x000f003f;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run",2,"D:P(A;CI;0
x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"
"MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time
Zones",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;S
Y)"
"MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx",2,"D:

P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;SY)"
"MACHINE\SOFTWARE\Windows 3.1 Migration
Status",2,"D:P(A;CI;0x000f003f;;;DA)(A;CI;0x00020019;;;AU)(A;CI;0x000f003f;;;C
O)(A;CI;0x000f003f;;;SY)"
"MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg",2,"D
:P(A;CI;0x000f003f;;;DA)(A;CI;0x000f003f;;;SY)"

[File Security]
"%SystemRoot%\SendTo",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;A
U)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"
"%SystemRoot%\Temporary Internet
Files",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff
;;;CO)(A;CIOI;0x001f01ff;;;SY)"
"%SystemRoot%\History",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;A
U)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"
"%SystemRoot%\COOKIES",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;
;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"
"%SystemRoot%\Help",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(
A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"
"%SystemRoot%\Security",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;S
Y)"
"%SystemDirectory%\Regedt32.cnt",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x00
1f01ff;;;SY)"
"%SystemDirectory%\Regedt32.hlp",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x00
1f01ff;;;SY)"
"%SystemDirectory%\Regedt32.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x00
1f01ff;;;SY)"
"%SystemDirectory%\Rexec.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f0
1ff;;;SY)"
"%SystemDirectory%\Rsh.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff
;;;SY)"
"%SystemDirectory%\Rcp.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff
;;;SY)"
"%SystemDirectory%\Ntbackup.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x00
1f01ff;;;SY)"
"%SystemDirectory%\Rdisk.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f0
1ff;;;SY)"
"%SystemDrive%\pagefile.sys",1,"D:P(A;CIOI;0x001200a9;;;SY)"
"%SystemRoot%\Regedit.exe",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;
;;SY)"
"%SystemDrive%\NTReskit",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;
CO)(A;CIOI;0x001f01ff;;;SY)"
"%SystemDrive%\Autoexec.bat",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x00120
0a9;;;AU)(A;CIOI;0x001f01ff;;;SY)"
"%SystemDrive%\boot.ini",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY
)"

"%SystemDrive%\Ntdetect.com",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"
"%SystemDrive%\Msdos.sys",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;AU)(A;CIOI;0x001f01ff;;;SY)"
"%SystemDrive%\Config.sys",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;AU)(A;CIOI;0x001f01ff;;;SY)"
"%SystemDrive%\ntldr",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"
"%SystemDrive%\Io.sys",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;AU)(A;CIOI;0x001f01ff;;;SY)"
"%SystemRoot%\Profiles",1,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;CIOI;0x001f01ff;;;SY)"
"%SystemDrive%\Win32app",1,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;CIOI;0x001f01ff;;;SY)"
"%SystemDrive%\Users",1,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;S-0x1-0x000000000005-0x15-0x3b1e46f5-0x69bf70fb-0x253b7c20-0x200)(A;CIOI;0x001f01ff;;;SY)"
"c:\boot.ini",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"
"c:\ntdetect.com",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"
"c:\ntldr",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"
"c:\autoexec.bat",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;AU)(A;CIOI;0x001f01ff;;;SY)"
"c:\config.sys",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;AU)(A;CIOI;0x001f01ff;;;SY)"
"%SystemDrive%\Program Files",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"
"%SystemRoot%\repair",2,"D:P(A;CIOI;0x10000000;;;DA)(A;CIOI;0x10000000;;;SY)"
"%SystemDirectory%\config",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"
"%SystemDirectory%\repl\import",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001301bf;;;RP)(A;CIOI;0x001f01ff;;;SY)"
"%SystemDirectory%\repl\export",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001200a9;;;RP)(A;CIOI;0x001f01ff;;;SY)"
"%SystemDrive%",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"
"%SystemDrive%\Temp",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001201bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"
"%SystemRoot%\$NtServicePackUninstall$",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001f01ff;;;SY)"
"%SystemDirectory%",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001200a9;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"

"%SystemRoot%",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;;0x001201bf;;;AU)(A;CIOIIO;
0x001200a9;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"
"%SystemDirectory%\spool\Printers",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x00
1301bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001301bf;;;RP)(A;CIOI;0x001f01ff
;;;SY)"
"%SystemRoot%\nsreg.dat",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001301bf;;;
AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"
"%SystemRoot%\drwtsn32.log",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001301
bf;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"
"%SystemRoot%\mapiuid.ini",2,"D:P(A;CIOI;0x001f01ff;;;DA)(A;CIOI;0x001301bf
;;;AU)(A;CIOI;0x001f01ff;;;CO)(A;CIOI;0x001f01ff;;;SY)"

[Service General Setting]
Schedule,4,"D:(A;;0x000200ad;;;DA)(A;;0x000201fd;;;SY)S:(SA;FA;0x000f01ff;;;
WD)"

[Privilege Rights]
SeAssignPrimaryTokenPrivilege =
SeAuditPrivilege =
SeBackupPrivilege = Administrators,Backup Operators,Server Operators
SeChangeNotifyPrivilege =
SeCreatePagefilePrivilege = Administrators
SeCreatePermanentPrivilege =
SeCreateTokenPrivilege =
SeDebugPrivilege =
SeIncreaseBasePriorityPrivilege = Administrators
SeIncreaseQuotaPrivilege =
SeInteractiveLogonRight = Administrators,Backup Operators,Account
Operators,Print Operators,Server Operators
SeLoadDriverPrivilege = Administrators
SeLockMemoryPrivilege =
SeMachineAccountPrivilege =
SeNetworkLogonRight = Administrators,Authenticated Users
SeProfileSingleProcessPrivilege = Administrators
SeRemoteShutdownPrivilege = Administrators,Server Operators
SeRestorePrivilege = Administrators,Backup Operators,Server Operators
SeSecurityPrivilege = Administrators
SeShutdownPrivilege = Administrators,Account Operators,Backup
Operators,Print Operators,Server Operators
SeSystemEnvironmentPrivilege = Administrators
SeSystemProfilePrivilege = Administrators
SeSystemTimePrivilege = Administrators,Server Operators
SeTakeOwnershipPrivilege = Administrators
SeBatchLogonRight =
SeServiceLogonRight =
SeTcbPrivilege =