



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Securing Windows and PowerShell Automation (Security 505)"  
at <http://www.giac.org/registration/gcwn>

**Andrew Berdahl**  
**Practical Assignment for GIAC Certification**

This document is written as a practical assignment for passing the GIAC certification in Windows NT 4.0 security. The goal of the document is to present a method of initially preparing a newly created Windows NT 4.0 Primary Domain Controller for auditing in a medium secure environment. The paper is in three parts: (1) The preparation of the new server for auditing, (2) The enabling of auditing, and (3) The creating of batch files to monitor and review the logs created by the auditing process. Keep in mind that there are many aspects to NT security but that the focus here is on the auditing process. The paper assumes that the reader has routine familiarity with the administration of Windows NT 4.0 Server.

**Preparing the server for auditing**

**NTFS**

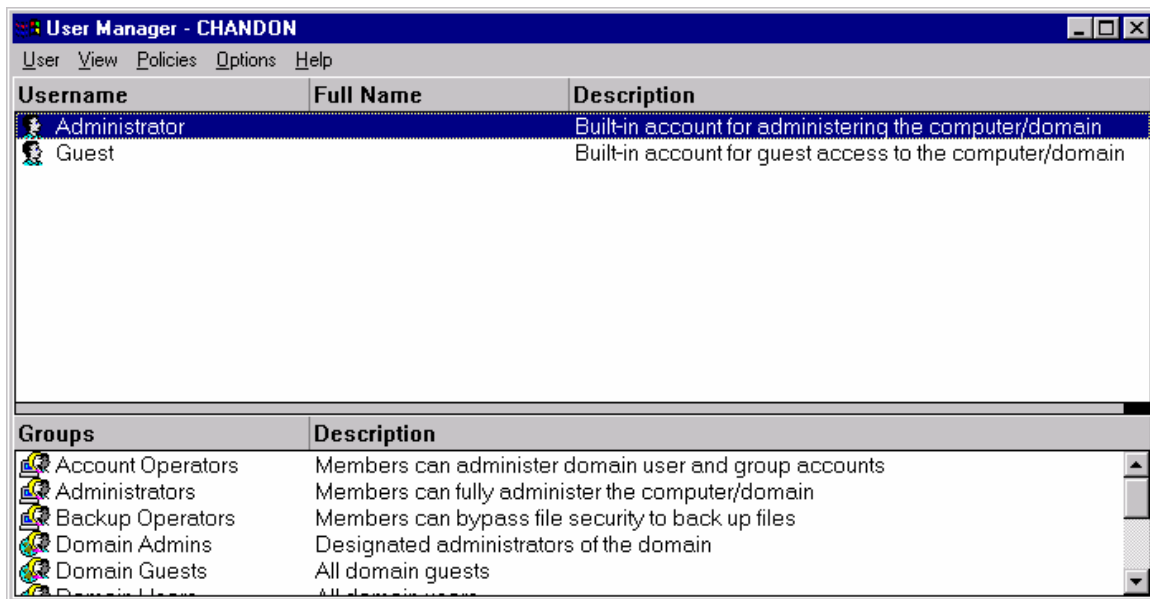
When installing the server make sure that all partitions are formatted with NTFS. It is somewhat “fashionable” to format the system and/or boot partitions as FAT, the thinking being that if the OS crashes the administrator can at least boot with a DOS diskette and get to the C: drive to run diagnostics or replace files. By formatting these partitions as FAT one compromises the ability to do any secure auditing of the OS in any way. But with the judicious maintenance of an Emergency Repair Disk, the use of Last Known Good, and a sound backup strategy, the NT administrator should never require FAT on any NT server. As another precaution, a second instance of NT Server can be installed on the same drive and an NT boot diskette created with the boot.ini file pointing to this second installation. If the original installation fails, the server can be booted into the second installation. From here, either the registry from the initial installation can be repaired or a good tape backup can be restored.

**Service Packs and Hotfixes**

Be sure the latest NT Service Pack is installed. Download any appropriate late patches and hotfixes from <http://corporate.windowsupdate.microsoft.com>.

**Protect the Built-in Accounts**

Password guessing is perhaps the most common method of gaining illicit access to a computer or network. There are two built-in accounts that come with NT: Administrator and Guest (Figure 1).

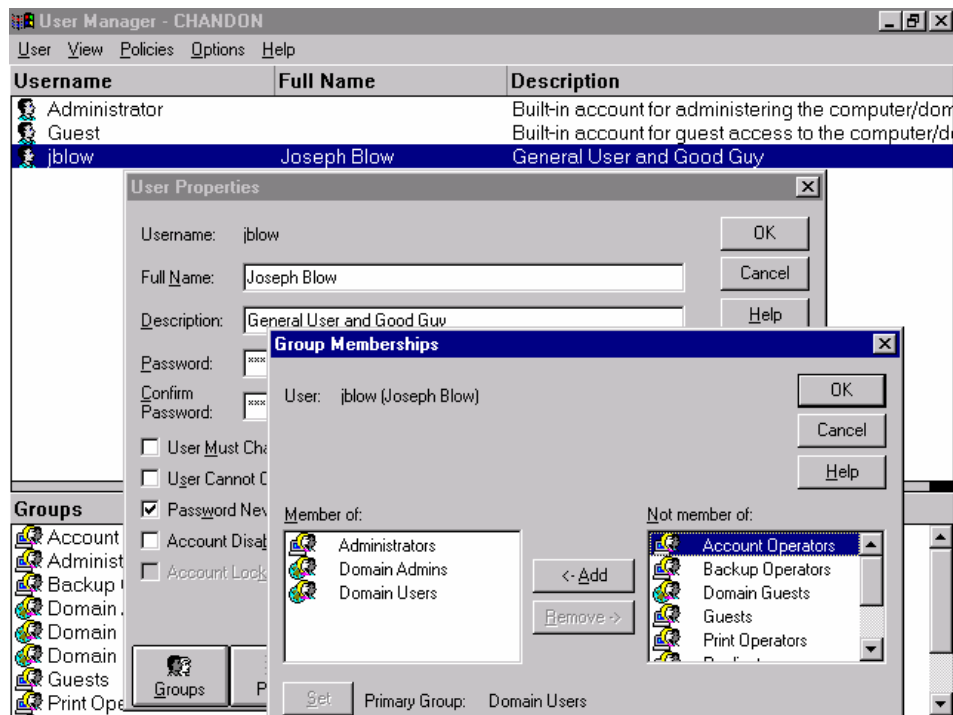


**Figure 1. The Default Built-in NT Accounts.**

Neither account can be deleted. So, because of the power inherent in the Administrator account and the potentially universal access available to the Guest account, these two accounts need special attention and protection when setting up auditing.

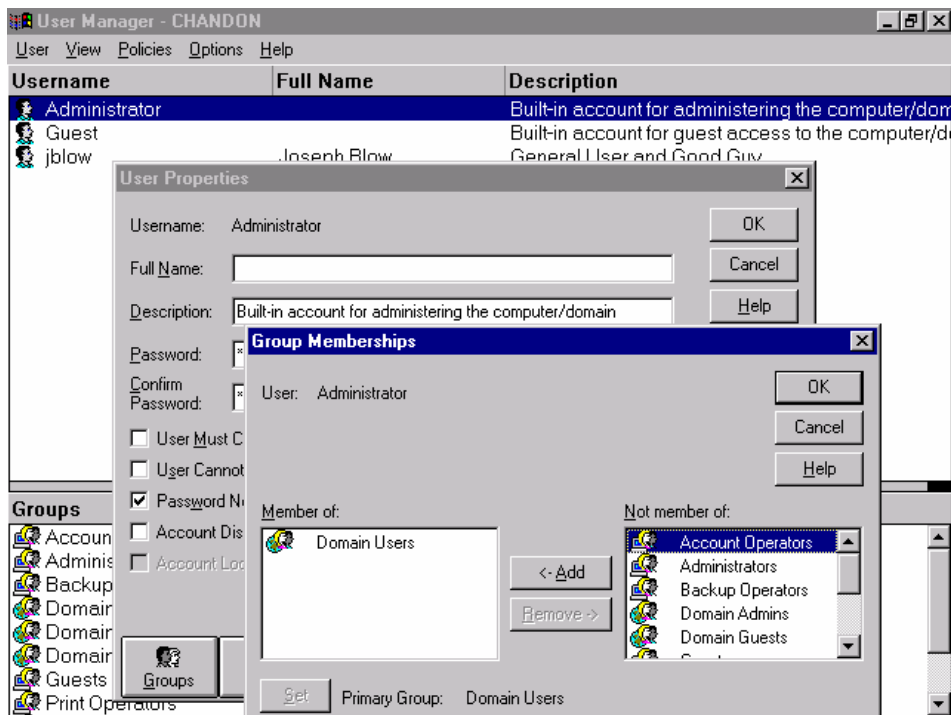
#### Administrator Account:

There are several options available to help protect the Administrator Account. The first option is to rename the Administrator account and then copy it, making the copied account name "Administrator." This should be done in this order to preserve the description field for the Administrator account that is longer than the standard default of 48 characters. Now change the description on the original account and apply a very strong password on the account (Figure 2).



**Figure 2. Copied Administrator Account with Admin Privileges.**

Remove all rights and permissions from the copied Administrator account and remove it from the Administrators and Domain Admins global groups. This sets up the Administrator account as a “honeypot” account, which can be useful during auditing, as we will see later. (See Figure 3.)



**Figure 3. Copied Administrator Account With No Privileges**

A second option to help protect the Administrator account from password guessing is the NT Resource Kit utility called Passprop. By default, the Administrator account cannot be locked out, even with Account Policies set to lock out accounts. Passprop will allow the Administrator account to be locked out just as any other account but still allow the Administrator the ability to logon interactively to a domain controller where the account can be re-enabled (Figure 4).

```

C:\WINNT\System32\cmd.exe

C:\>passprop help
Displays or modifies domain policies for password complexity and
administrator lockout.

PASSPROP [/complex] [/simple] [/adminlockout] [/noadminlockout]

    /complex          Force passwords to be complex, requiring passwords
                      to be a mix of upper and lowercase letters and
                      numbers or symbols.

    /simple            Allow passwords to be simple.

    /adminlockout     Allow the Administrator account to be locked out.
                      The Administrator account can still log on
                      interactively on domain controllers.

    /noadminlockout   Don't allow the administrator account to be locked
                      out.

Additional properties can be set using User Manager or the NET ACCOUNTS
command.

C:\>passprop /adminlockout
Passwords may be simple
The Administrator account may be locked out except for interactive logons
on a domain controller.

C:\>_

```

Figure 4. The Passprop Command Line Utility

#### Guest Account:

The domain Guest account is disabled by default after installation of NT Server 4.0. Make sure that it stays disabled and also be sure to check off “User Cannot Change Password” and “Password Never Expires” and apply a strong password on the account (Figure 5).

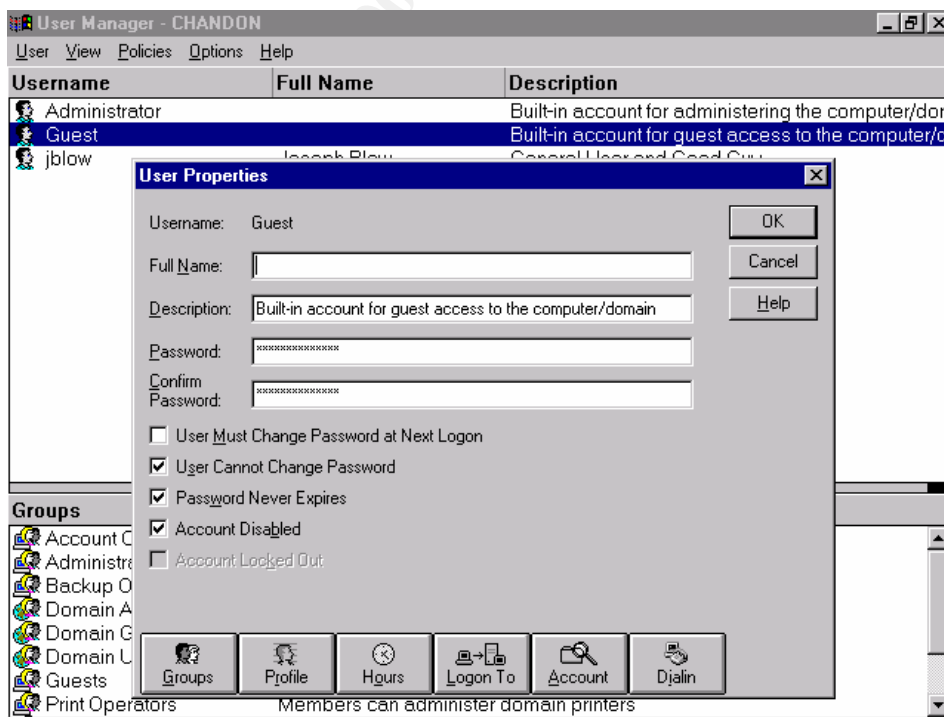


Figure 5. Disabled Guest Account

## Account Policies

For auditing to be effective there need to be some parameters set on user accounts in which to audit. There are several options possible to set these account parameters or policies. These include configuring the Account Policy from User Manager for Domains, setting up Passfilt.dll in the registry, or using third-party utilities such as Password Padlock and Password Appraiser.

Use Account Policy from User Manager for Domains to set account policies globally for all domain accounts (Figure 6). Under the Policies menu in UMD, select Account.

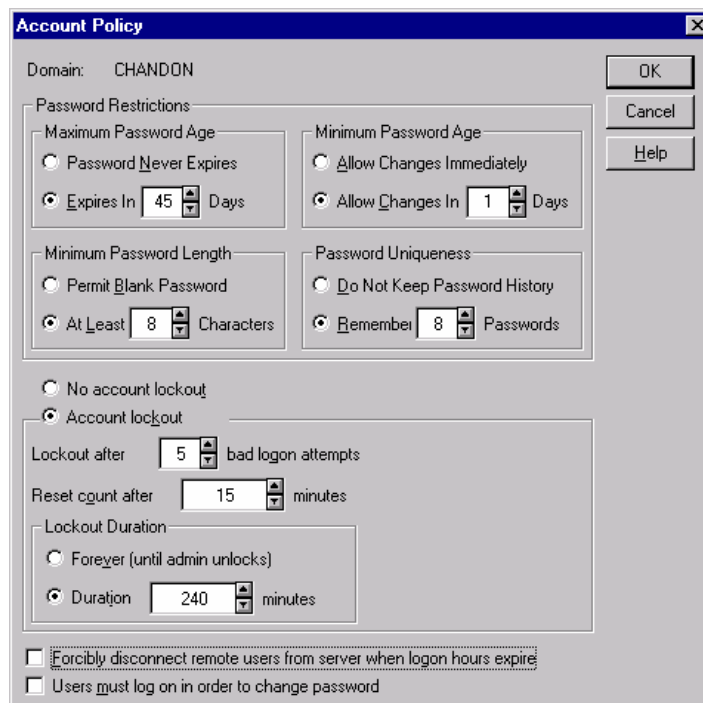


Figure 6. The Account Policy from User Manager for Domains.

**Maximum Password Age** determines how long account passwords are active before they expire. For a medium-security network set this value for no more than 45 to 90 days.

**Minimum Password Age** determines how long a user account is forced to retain a new password. For a medium-security network set this to at least 1 day. This will keep users from rapidly changing their passwords to get back to one that they want. The only “gotcha” with this is that users who logon with an account created the same day will not be able to change their passwords when “User Must Change Password at Next Logon” is set in the account properties.

**Minimum Password Length** determines the minimum allowable password length for all passwords. For a medium-security network set this value to at least 8 characters.

**Password Uniqueness** tells the server whether to keep a history of previously used passwords. For a medium-security network set this value to remember

between 8 to 13 prior passwords.

**Account Lockout** sets up lockout parameters to deter repeated illegal logon attempts. Set the Lockout After x Bad Logon Attempts to no less than 5 attempts, the Reset Count to 15 minutes, and the Lockout Duration to no less than 240 minutes (4 hours).

(All above values are those suggested by SANS Securing Windows NT Step-by-Step)

In addition to manually setting password values in the Account Policy window, the administrator should enable password filtering to require complex passwords when a user attempts to change his or her password. This can be done by adding an entry for Passfilt.dll to the Notification Packages in the registry (Figure 7). Passfilt.dll, which has been included with NT since SP2, is not set in the registry by default. You must set this manually. Once this is set, all password changes made from the security subsystem using Ctl+Alt+Del will require that passwords have at least six characters and that they cannot contain any part of the username or any common words such as "password." They also will be required to have three of the following four types of characters: uppercase letters, lowercase letters, numbers, and special characters such as punctuation marks. The registry location for Passfilt is:

Hive: HKEY\_LOCAL\_MACHINE  
Key: \System\CurrentControlSet\Control\Lsa  
Value Name: Notification Packages  
Value Type: REG\_MULTI\_SZ  
Value Data: PASSFILT

If there is already an entry for FPNWCLNT and there are no NetWare clients on the network then FPNWCLNT can safely be deleted. Otherwise, PASSFILT should be placed under FPNWCLNT.



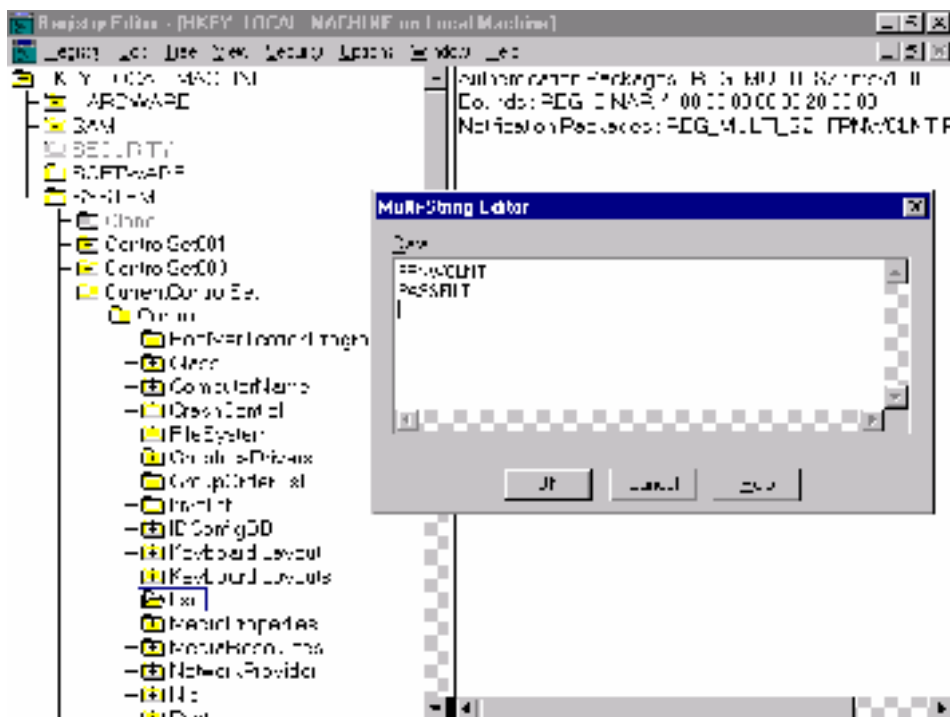
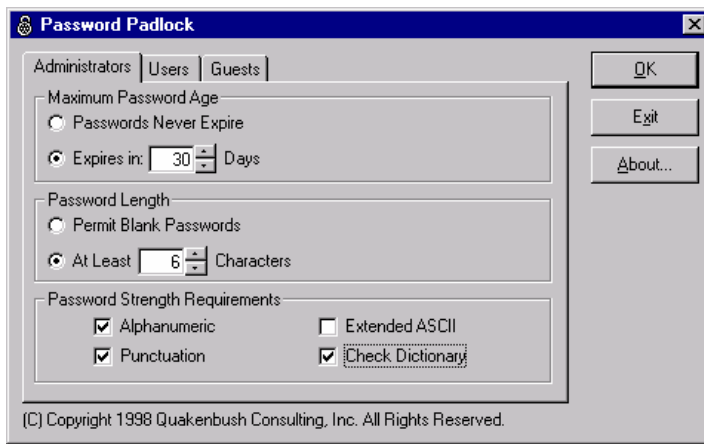


Figure 7. Setting Passfilt in the Registry.

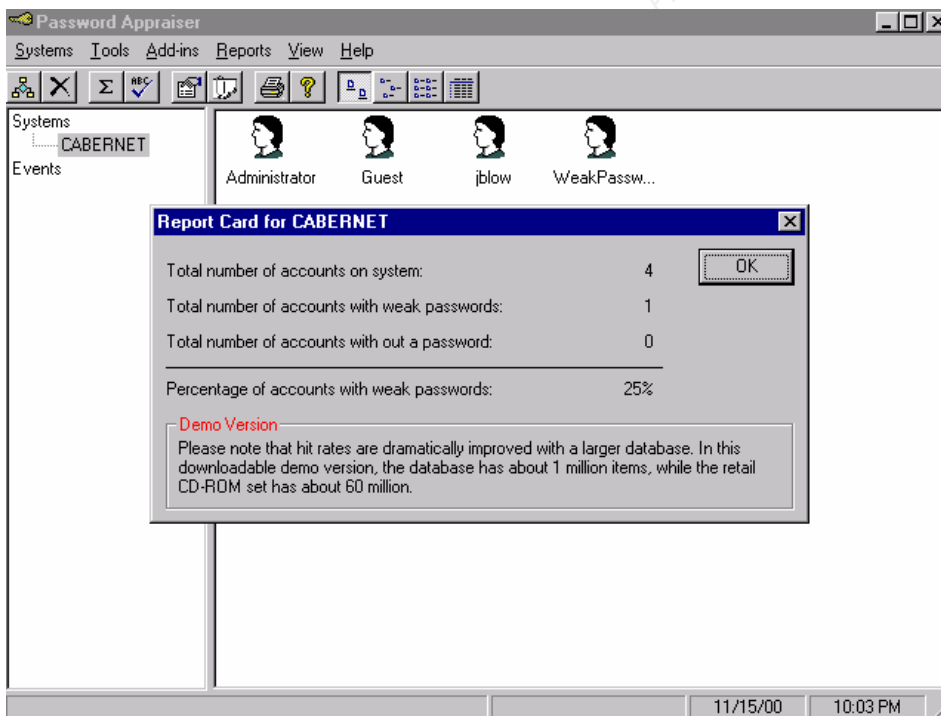
**Warning:** If Passfilt is set but there are no password restrictions set in the Account Policy, when the user goes to change their password they may get a message stating that the password must be “0” characters long. To resolve this be sure that there is a minimum password length of six characters set in the Account Policy. (See TechNet article Q196465.)

Third-party tools such as Password Padlock and Password Appraiser from Quakenbush (<http://www.Quakenbush.com>) can be used to set password strength levels for different types of accounts and can then monitor the SAM database on all domain controllers for weak passwords. Password Padlock will allow you to set separate password policies on Administrators, Guests, and Users accounts (Figure 8).



**Figure 8. Password Padlock from Quakenbush.**

Password Appraiser will scan all accounts in the SAM database on all domain controllers and report any weak or “cracked” passwords based on how the restrictions have been set in Password Padlock or the Account Policy (Figure 9). Scanning can be scheduled regularly and if weak passwords are detected, alerts to an administrator can be set.



**Figure 9. Password Appraiser from Quakenbush**

### Hidden Admin Shares

Consider removing the following hidden admin shares: C\$, D\$, ... <driveletter>\$, Admin\$. There is one other default hidden share, RepL\$, but this must not be removed because it is needed for replication. If administrators need these shares for administrative work, batch file use, etc., then new hidden shares names that look generic can be created

for that purpose. Be sure that only the Administrators group is granted share permissions to these new hidden share names.

### The Everyone group

As long as you are running SP3 for NT 4.0 you should remove the Everyone group from all share permissions and NTFS permissions on the local drives and replace the Everyone group with Authenticated Users. Keep the same permissions for Authenticated Users as were set for the Everyone group. The reason for doing this is that it is possible for an intruder to create what is known as a Null Session to a remote server. In Figure 10, a user without domain credentials tries to use a “net view” command to list the share names on the computer named Cabernet but is refused. The user then creates a null session using a “net use” command. Now the “net view” command can be repeated successfully. Once this is done the user will be able to map drives to these shares and have all permissions available that are assigned to the Everyone group.

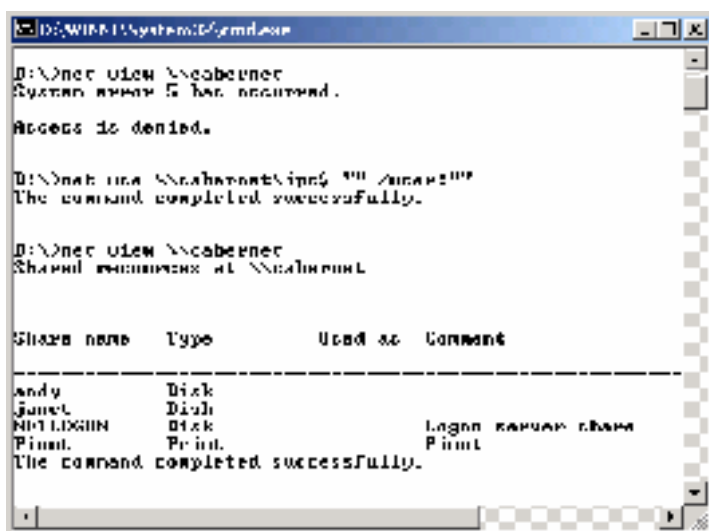


Figure 10. Creating a Null Session

By replacing the Everyone group with Authenticated Users, the user will be prevented from successfully accessing a remote server when using a Null Session. The following is an excerpt from the TechNet article Q132679:

A null session is only established when there are no credentials for a process to start under (no user name or password). Typically, only the operating system itself runs as system.

On the local machine, the operating system is known as:

```
Default Owner:  Administrators local group
User:           System pseudo group - local group scope
Groups:         Administrators local group
                Everyone pseudo group - local group scope
```

When this context is used to access the network, a null session is

used. This produces the following context on remote machines:

```
Default Owner:  Everyone
User:           Everyone
Groups:         AnonymousLogon pseudo group - local group scope
                Network pseudo group - local group scope
```

Only three identifiers can provide the null session access (Everyone, AnonymousLogon, and Network). The local system context and null session context have only the identifier Everyone in common. To configure Windows NT so that a service can access objects on its own machine directly, as well as over the network, use the Everyone identifier.

The default owners of these two contexts (as well as their default DACLs) are different. Any files you created in these contexts will be owned by Administrators. Any files you create through a null session will be owned by Everyone.

In addition to displaying shares on a remote server and mapping drives to those shares on which the Everyone group has permissions set, the null session will allow a user to display a list of user accounts for the domain using command line utilities such as NTUser from Pedestal Software and DumpSec from SomarSoft.

To block all null session activity to a remote server, an entry called RestrictAnonymous can be made in the registry of the server (Figure 11). The registry location is:

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

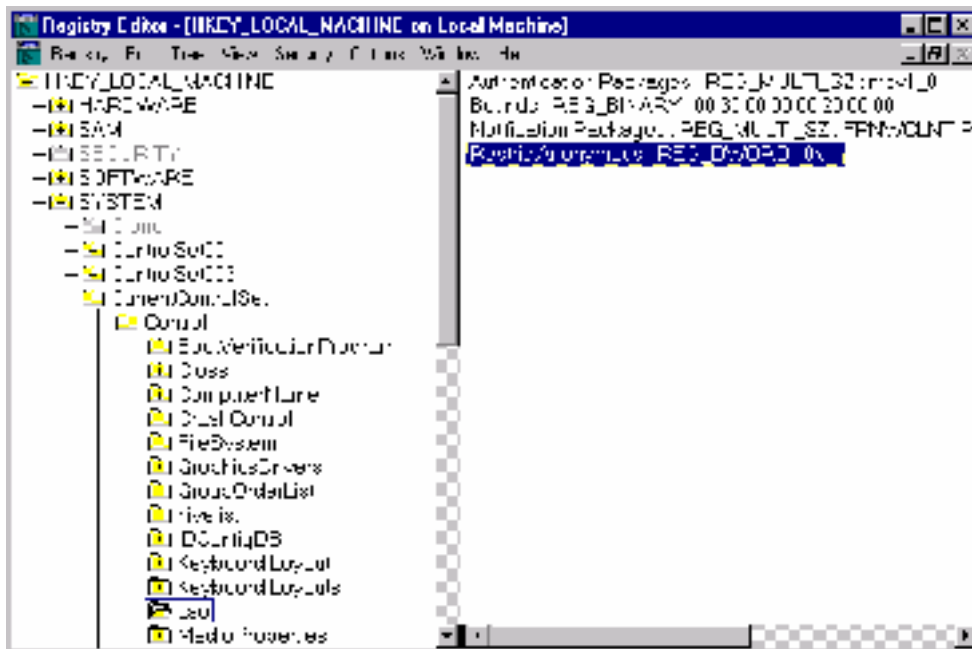


Figure 11. RestrictAnonymous Setting in the Registry.

### Protect the Event Logs

Auditing won't be worth anything if someone can get to the logs and delete them. So, make sure that the NTFS permissions for the folder that contains the event logs (\winnt\system32\config) are set so that only the local Administrators group and the System account have Full Control of the folder and its files. No other permissions should be set. Also, make sure that the setting for the User Right "Manage auditing and security log" is only granted to the Administrators group (the default setting).

### Log File Settings

Before Auditing is started, the settings for the audit log file, SecEvent.evt (found in the c:\winnt\system32\config folder) must be configured. This is done from within the Event Viewer in the Administrative Tools (Common) program group. Under the Log menu select "Log Settings..." (Figure 12). Select the Security log in the dropdown menu. Set the log size to something that will not fill quickly (4MB is suggested), and select "Do Not Overwrite Events". Click OK.

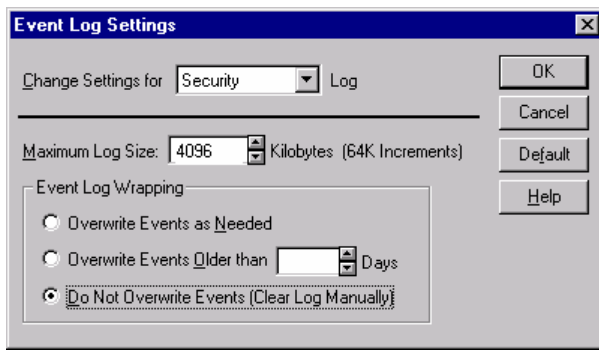


Figure 12. Configuring the Security Log Settings.

If “Overwrite Events as Needed” is selected then the log will not be useful for long term tracking of auditable events. “Overwrite Events Older than (x) Days” will also flush out valuable data from the log, although it will allow the log to fill which, when coupled with CrashOnAuditFail, creates some protection from intruders (see next section).

#### Crash Dump File and CrashOnAuditFail

If the audit log file is set to “Do Not Overwrite Events” or “Overwrite Events Older than (x) Days” and the log file fills by the actions of an intruder or by other wildly spinning events, then no more auditing is done but the operating system on the server continues allowing the intruder to work without being tracked. To prevent this from happening it is necessary to enable CrashOnAuditFail in the registry (Figure 13).

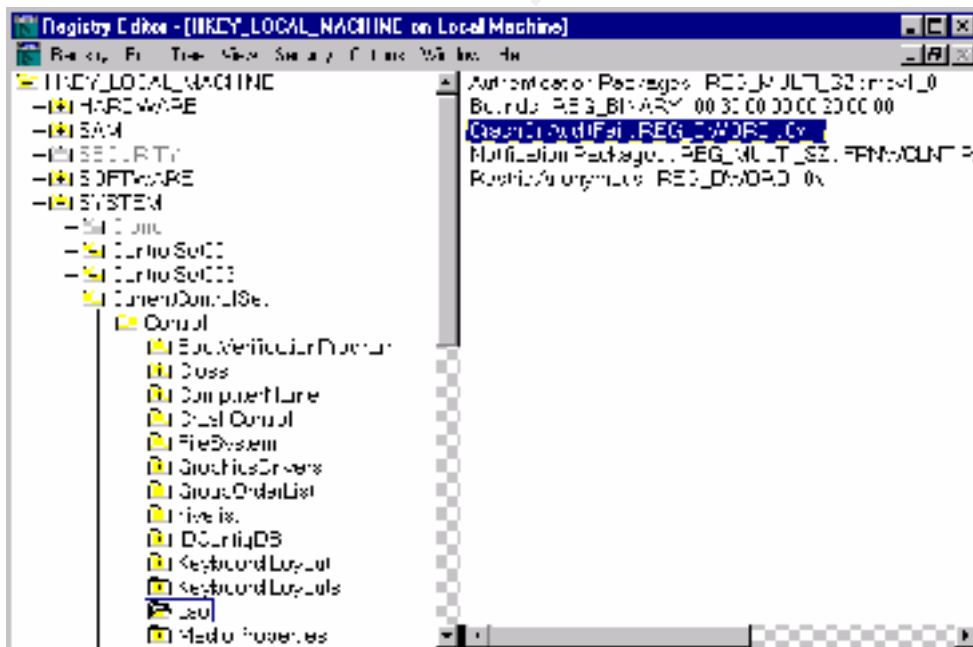
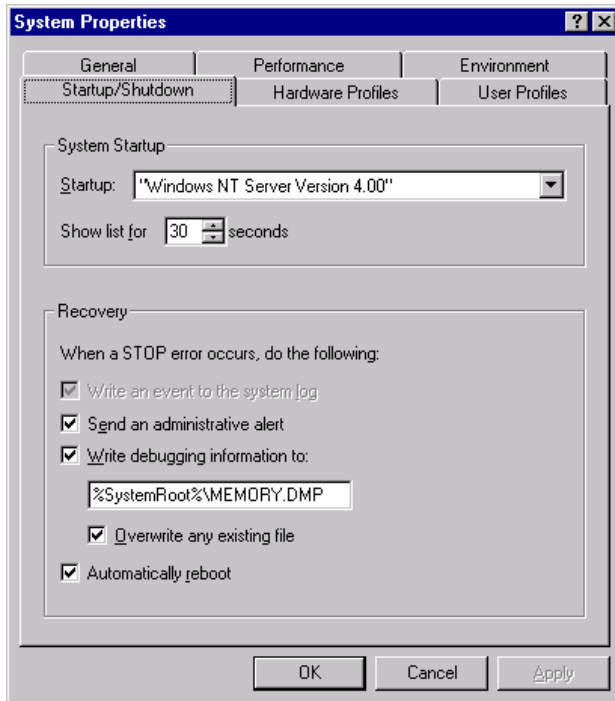


Figure 13. CrashOnAuditFail Setting in the Registry.

Once this is done and the log file fills, the server will “blue screen” with the following message:

```
STOP: C0000244 {Audit Failed}
An attempt to generate a security audit failed. (TechNet article
Q232564)
```

This will deny an intruder access to the server (along with everybody else in the company) until the server is rebooted and the log file is cleared. The above situation can be avoided by forcing the server to reboot after a crash. This is done by enabling the crash dump file in the System properties (Figure 14).



**Figure 14. Setting the Crash Dump file and Automatic Reboot.**

Notice that the option to “Write an event to the system log” is grayed out. With SP4 this option for NT Server became mandatory (Tips and Traps, Windows NT Magazine, Oct, 1999). It is still an option with NT Workstation. Keep in mind that when the crash dump file is enabled there must be enough disk space on the boot partition to allow for a memory dump in addition to any paging file that is on the same partition.

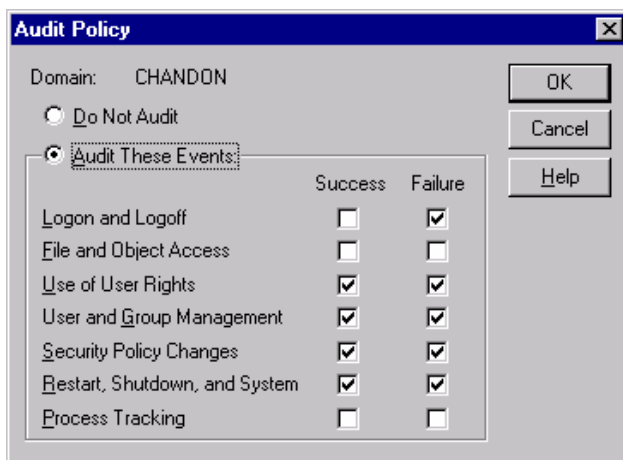
Once the audit log settings are made, and CrashOnAuditFail is set in the registry, and the crash dump file is enabled, there is one major “gotcha.” When the server reboots from a crash and if it is a PDC, the value setting in the registry for CrashOnAuditFail will automatically be set to 2. This setting will not allow anybody in the company to log onto the domain except for Domain Admins. This is by design as a security feature. In this event, users will receive the following error when attempting to log on:

```
You are not allowed to logon from this workstation. (TechNet
article Q155076)
```

The Helpdesk will start getting calls saying that nobody seems to be able to logon, but Domain Admins will see no problem. Unless someone remembers that CrashOnAuditFail needs to be reset to a value of 1 and the server rebooted, troubleshooting the problem can be frustrating.

## **Enabling Auditing**

Now that the server is prepared to start auditing, auditing needs to be enabled and configured so that events critical to the organization can be tracked. Auditing is enabled from within User Manager for Domains. Under the Policies menu select Audit. Click on “Audit These Events.”



**Figure 15. The Audit Policy from User Manager for Domains**

The following table will help you decide which events to audit. Keep in mind that, generally, failed events are more interesting to the administrator than successful events and that the more events that are audited the more resources are used on the server, slowing performance.

| Category                                       | Meaning   |
|--|---|
| Account Management (User and Group Management) | These events describe high-level changes to the user-accounts database, such as User Created or Group Membership Change. Potentially, a more detailed, object-level audit is also performed. (See the “Object Access” category, below).       |
| Detailed Tracking (Process Tracking)           | These events provide detailed subject-tracking information, such as program activation, handle duplication, and indirect object access.   |
| Logon/Logoff (Logon and Logoff)                | These events describe a single logon or logoff attempt, whether successful or unsuccessful. Included in each logon description is an indication of what type of logon (that is, interactive, network, or service) was requested or performed. |

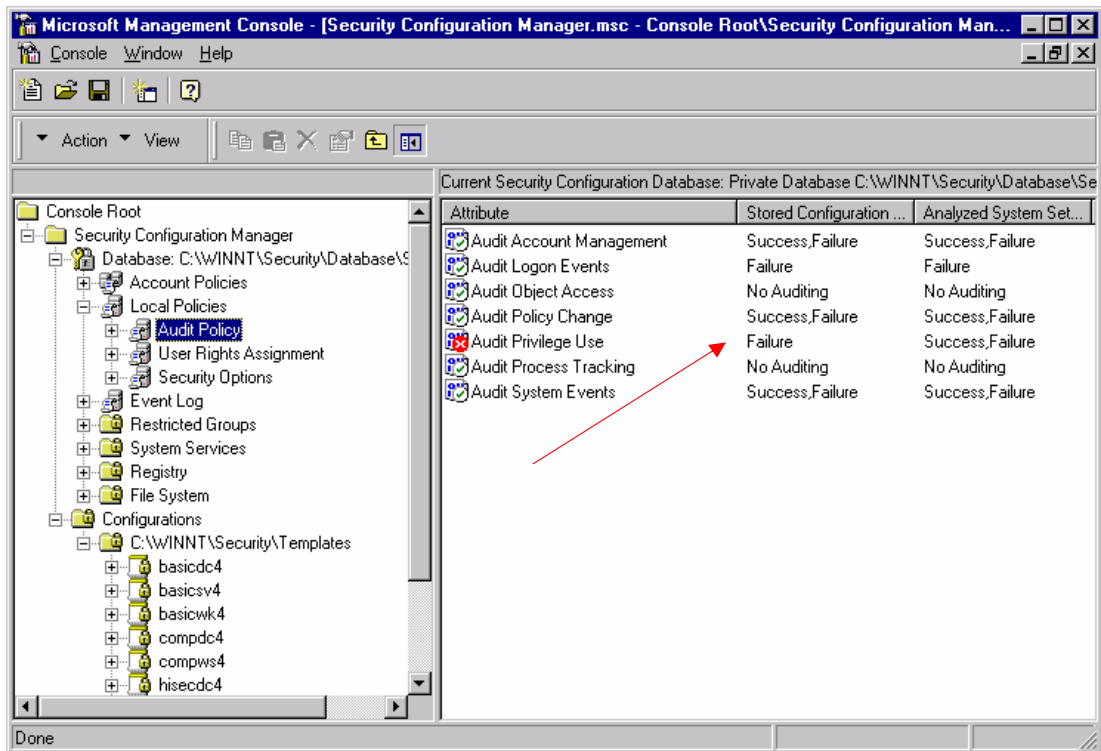


|  |  |
|--|--|
| Object Access (File and Object Access)       | These events describe both successful and unsuccessful accesses to protected objects including printers.   |
| Policy Change (Security Policy Changes)      | These events describe high-level changes to the security policy database, such as assignment of privileges or logon capabilities. Potentially, a more detailed, object-level audit is also performed. (See the “Object Access” category, above).                 |
| Privilege Use (Use of User Rights)           | These events describe both successful and unsuccessful attempts to use privileges. The category also includes information about when some special privileges are assigned. These special privileges are audited only at assignment time, not at the time of use. |
| System Event (Restart, Shutdown, and System) | These events indicate something occurred that affects the security of the entire system or audit log.  |

(From the Microsoft Windows NT Server Networking Guide, page 80)

#### The Microsoft Security Configuration Manager

An excellent tool for configuring auditing and many other aspects of NT Server and Workstation security is the Security Configuration Manager from Microsoft. This is a stand-alone snap-in for the Microsoft Management Console (MMC) that can be applied to NT Server and Workstation 4.0. It uses a graphical interface and comes with many preset templates of varying levels of NT security that can be applied to the servers and workstations on the network. The templates can be used as they are or modified for the specific network situation. Once they are applied, the administrator can monitor any discrepancies on the network and make changes on the spot. Notice that in Figure 16, there is a discrepancy in the audit policy between the stored configuration of the template and what is actually configured on the server. Here the administrator has a choice of changing the parameter in the template or using the preset parameter to configure the server's audit policy.



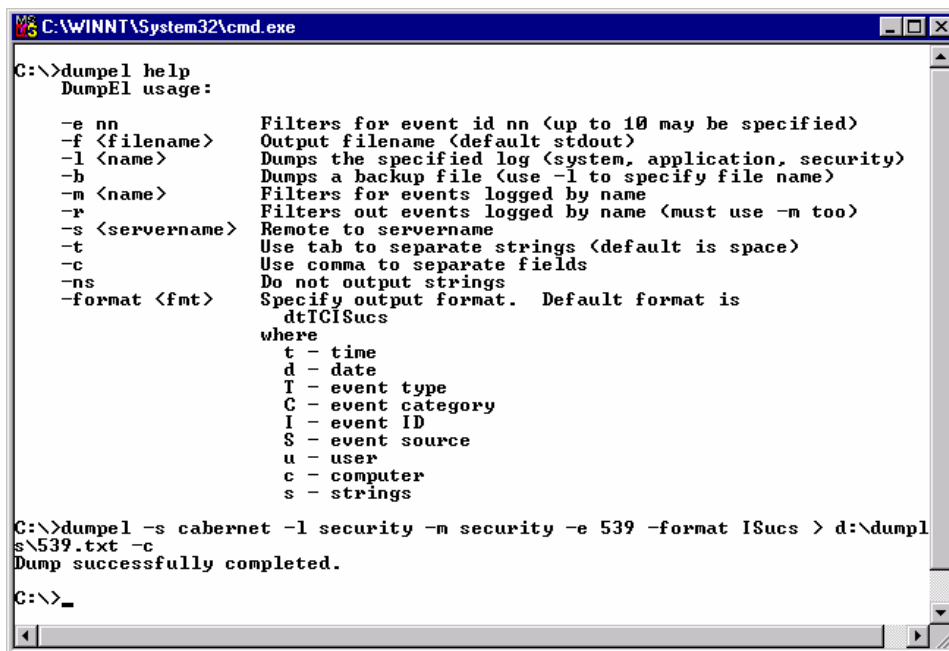
**Figure 16. Setting Auditing Parameters Using Security Configuration Manager.**

## **Creating Batch files to monitor the event logs**

### **Batch Files Using DumpEL**

Once auditing is enabled, the Event Viewer on the administrator's own workstation can be used to look at the logs on the server. This can be a daunting task because of the sheer number of entries that can be logged. The administrator will find it convenient to create batch files that will filter out specific Event ID's. The administrator should create batch files that will dump the contents of the security log file to folders that are remote from the server for daily reviewing and analysis. The administrator's own workstation is convenient for this purpose.

DumpEL is an NT Resource Kit command line utility that can be used to dump the security log file contents to a text file (Figure 17). It can also be set up to dump a particular Event ID from the log. Assuming that failed logon events are being audited, two of the events to monitor closely in the Event Viewer are Event ID 529 and 539. An Event ID 529 is logged when a user fails to logon either to the domain or interactively to a local workstation. An Event ID 539 is logged when a user account is locked out because it exceeded the number of bad logon attempts set in Accounts Policy. (See TechNet article Q171148.) By monitoring these two events daily, the administrator can track failed logons and account lockouts, both of which can expose intruder activity. In Figure 17, the DumpEL command is shown as it could be used in a batch file to dump Error 539 log entries.



```
C:\>dumpel help
DumpEl usage:

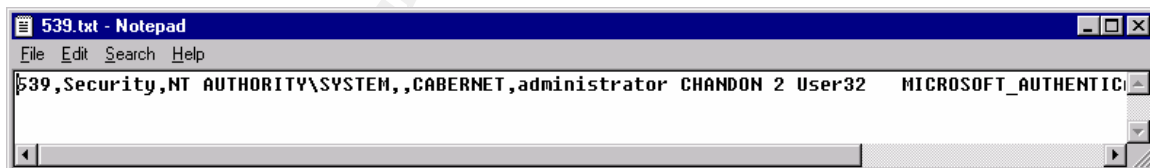
-e nn          Filters for event id nn (up to 10 may be specified)
-f <filename>  Output filename (default stdout)
-l <name>      Dumps the specified log (system, application, security)
-b            Dumps a backup file (use -l to specify file name)
-m <name>      Filters for events logged by name
-r            Filters out events logged by name (must use -m too)
-s <servername> Remote to servername
-t            Use tab to separate strings (default is space)
-c            Use comma to separate fields
-ns           Do not output strings
-format <fmt> Specify output format. Default format is
               dtIGISucs
               where
                 t - time
                 d - date
                 I - event type
                 C - event category
                 I - event ID
                 S - event source
                 u - user
                 c - computer
                 s - strings

C:\>dumpel -s cabernet -l security -m security -e 539 -format ISucs > d:\dumps\539.txt -c
Dump successfully completed.

C:\>_
```

Figure 17. Using DumpEL to Dump Event ID 539 – Account Locked Out.

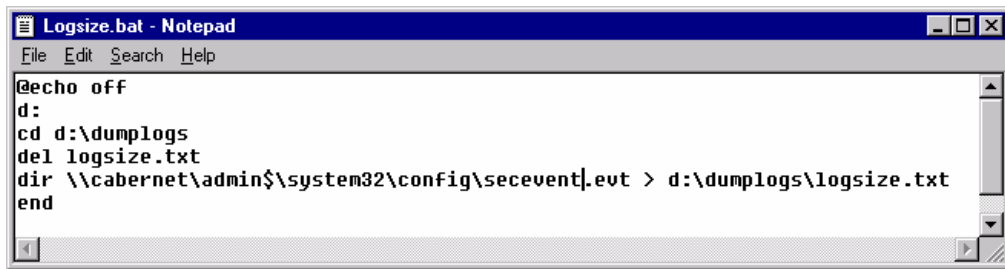
Notice that in Figure 18, the output of the previous DumpEL command reveals that the Domain Administrator account was locked out because Passprop was enabled earlier and the Administrator account password was entered incorrectly 5 times. The administrator can also see the name of the computer from which the failed logon was attempted (in this case, the PDC). This is an example of how to use the Administrator account as a honeypot account to detect when someone is trying to guess the Administrator account password. A similar batch file should be created to monitor Event ID 529 log entries, the failed logon attempts, or any other Event ID that the administrator wants to monitor.



```
539,Security,NT AUTHORITY\SYSTEM,,CABERNET,administrator CHANDON 2 User32 MICROSOFT_AUTHENTIC...
```

Figure 18. Output from DumpEL Command.

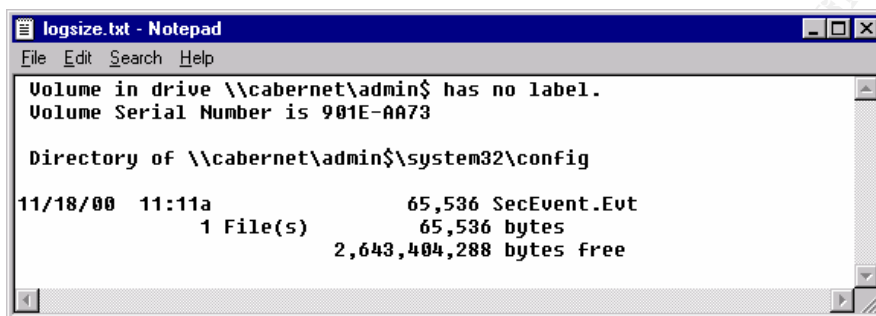
Because the event log is set to not overwrite events but to log events until either the log fills or the administrator clears the log, it is very important to monitor the log size daily. This can be done using the Dir command in a batch file and redirecting the output to a text file (Figure 19).



```
@echo off
d:
cd d:\dumplogs
del logsize.txt
dir \\cabernet\admin$\system32\config\secevent|.evt > d:\dumplogs\logsize.txt
end
```

Figure 19. Using a Batch File to Monitor the Size of the Event Log.

The output of the batch file is shown in Figure 20. The administrator would normally include the other two log files (Application and System logs) in Logsize.bat, but only the Security Log is shown for clarity.



```
Volume in drive \\cabernet\admin$ has no label.
Volume Serial Number is 901E-AA73

Directory of \\cabernet\admin$\system32\config

11/18/00  11:11a           65,536 SecEvent.Evt
              1 File(s)          65,536 bytes
              2,643,404,288 bytes free
```

Figure 20. Output of Logsize.bat

## **Conclusion**

By following the steps presented in this paper, the administrator can initially prepare a new Primary Domain Controller running NT Server 4.0 for the purposes of auditing. The security level applied is roughly for a medium secure network. From this point the administrator can use batch files to monitor the security logs created by auditing and can use such tools as Security Configuration Manager to fine-tune the permissions set in the registry and file system as needed so that the auditing process will produce relevant data.