Global Information Assurance Certification Paper

File Auditing in Microsoft Windows NT 4.0

GIAC Certification
Windows NT Security
Practical Application Requirement

SANS Security 2001
New Orleans, LA

K. Nolan Carter

[THIS PAGE INTENTIONALLY LEFT BLANK]

File Auditing in Windows NT

[THIS PAGE INTENTIONALLY LEFT BLANK]

Table of Contents

[THIS PAGE INTENTIONALLY LEFT BLANK]

Objective

The objective of this paper is to familiarize the reader with a process of determining an appropriate file auditing scheme for any Windows NT 4.0 system. Emphasis will be placed on utilizing Windows NT 4.0 auditing capabilities, limiting use of third-party utilities, reviewing system security needs, establishing an appropriate auditing policy, defining appropriate auditing functions, and demonstrating the implementations of these functions. This objective will be achieved through the use of a general case study designed to help the reader become familiar with steps he should follow when establishing a security plan for his own system(s). In this paper, the reader will become familiar with the implementation of file auditing, how to determine which events should be audited, and how to determine if auditing the success and failure of each event is necessary. This paper can be used as a step by step guide for file auditing, as it provides illustrated instructions for using the Event Viewer, and examples of viewing and interpreting security logs, as well as a demonstration of archiving the security logs.

Overview

A computer security standard must be carefully reviewed and decided upon prior to implementation. This standard will vary greatly from organization to organization. Each organization must assess its own needs, and determine an appropriate balance between functionality and security for itself. At a minimum an organization should consider the following:

Access Policies -	Who is allowed to use an account
	Password Requirements
	Proper and Improper Use of Systems
	Rules and Guidelines for Usage
	Consent to Monitoring
	Group Membership
	File Permission
System Policies -	Installation Policy
	Determine Essential/Non-Essential Services
	Upgrade Policy
	Backup Policy
	System Monitoring
	Security Audits
Breech Recovery Policies-	Restoration of Data
	Incident Handling
	Intruder Prosecution

Before deciding upon how to utilize the customizable features of your Windows NT system, the organization must adopt a set of computer use and security policies. These policies should be established prior to the deployment of Windows NT systems on the network. It is most effective if an organization has reviewed and printed guidelines and/or a "tried and true" outline for each workstation. Also an organization should incorporate the "General Security Guidelines" as outlined in "Windows NT Security – Step by Step" published by the SANS Institute as a best practice guideline. These guidelines embrace the least privilege principle, carefully planned groups and permissions, limited trust, securing the Remote Access Service (RAS), limiting

access to the Network Monitor, using third-party authentication, and keeping the system up to date.

Microsoft Windows NT 4.0 is capable of incorporating many levels of security, from no security to the C2 security level as defined by the National Computer Security Center (NCSC) publication Department of Defense Trusted Computer System Evaluation Criteria. There are a number of customizable security features in Microsoft Windows NT including: User Accounts, password permissions, File and Directory Protection, registry protection, and printer protection just to name a few.

An unlimited number of user accounts that can be used individually or by adding them to groups and enforcing a group policy. By assigning privileges to these user accounts it is possible to permit or deny access to any computer resource.

Password permission is also incorporated with Windows NT and can be used to restrict access to resources and accounts. It is possible to customize the password policy to fit the specific organizational need.

File and directory protection can be established on a by-file or by-directory basis and can be implemented alone or used in correlation with user account and guest account security.

Registry protection is customizable and should be enforced since the registry is the repository of all system configurations.

Printer protection can be customized to prevent certain users from printing to specific devices for specific periods of time or permanently.

Monitoring performance helps the system administrator fine tune the system and it is capable of warning of approaching problems.

Auditing is another customizable capability of Windows NT. Security auditing is disabled by default and must be enabled before it is possible to track security related events. Security auditing provides many ways of tracking account use and object access to such as printers, file and directory sharing, and file and folder access. Auditing can also be used to track other critical system security events such as the restart and shutdown of the system, successful and failed logon attempts, and other security events. Each organization should create its own unique level of system security to fit the needs of the company or system.

Defining an Audit Policy

An audit policy is a very important part of Windows NT security. When used correctly it can provide information on a wide range of security events. It can help the system administrator determine items such as: common trends; authorized and unauthorized access to the system and data; changes to user accounts and groups; normal use or the abuse of files, shares, and printers; use of system level processes; system events like start-up and shut-down. When determining an audit policy the system administrator should consider the following, at a minimum:

1. Use of File and Directory Resources
2. Logon/Logoff Events
3. Shutdown and Restart of the System
4. Changes to Users and Groups
5. Security Policy Changes

When making decisions about whether or not to audit the events listed above, determine the need or want for auditing the success and/or failure of each event. Success will tell how often these events take place and will provide a baseline for appropriate activity. If the system administrator plans on auditing the success of events in order to establish "trends" of appropriate activity, then a plan for archiving the event logs should be established. The failure of these events will help the system administrator determine intrusion attempts and security breeches.

Audit Policy - Audit Classes Defined

The audit classes available for auditing are shown in the Audit Policy window [Fig. 1]. Clicking on "success" or "failure" for each class, the system administrator can determine what events will be audited. Each class is defined below to assist in the selection of the appropriate audit factors.

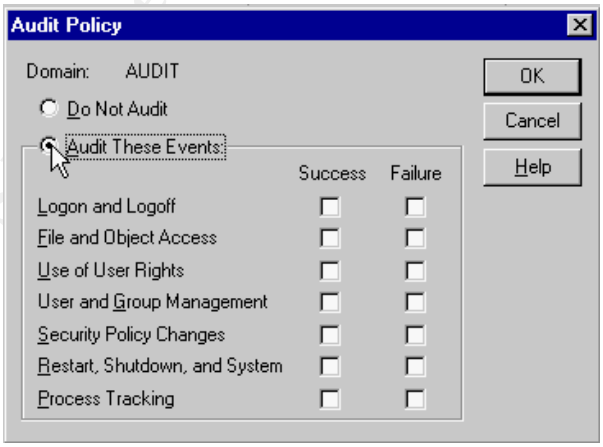

Figure 1 – Audit Policy Window

Logon and logoff – Success of this class provide a baseline of appropriate logon and logoff events. User trends such as working schedules can be established in order to assist in determining intrusion attempts outside the normal range of activity. Auditing the failures of this class is a method of identifying repeated intrusion attempts to the account.

File and Object Access – Success and failures of this class provide a baseline of appropriate activity with files, folders, printers, and/or shares. File and object access auditing will provide information on: displaying file or folder names, displaying data, file or directory attributes, changes to directory attributes, displaying file and owner permissions, creating files or subdirectories, changing the file or the files attributes, access to subdirectories, the execution of files, deleting of files or directories, changing file or directory ownership, or changing file or directory permissions. It can also provide information on the use of specific printers. Any changes made to files can be tracked and logged. This is especially helpful when proprietary or sensitive information resides on a system.

Use of User Rights – Success and failures of this class provide information on the use and misuse of backing up files and directories, shutting down the computer, logging on interactively, and changing the system times as defined by Windows NT. Caution: Auditing user rights can quickly eat up system resources since most normal activities involve the use of user rights. [Fig. 2 and Fig. 3]

User and Group Management – Success and failures of this class provide information on the addition, modification, or deletion of users and groups.

Security Policy Changes – Success and failures of this class provide information on changes to the auditing policy or the reassignment of user rights. It is suggested that this be audited since changes to this class will only occur rarely.

Restart, Shutdown, and System – Success and failure of this class provide information on system shutdown, booting, or any other event that affects system security or the security log.

Process Tracking – Success and failure of this class provide information on program activation and other important system-level information about processes.

User Right	If you have this right, Then you are able to...	Groups Holding by default
Basic User Rights		
Access this computer from the network	Use shared resources via the network	Everyone, Admins Power Users
Add workstations to domain	Define a system as part of the domain	None
Backup files and directories	Access or modify any file or directory on the system, regardless of its ACL	Administrators Backup Operators Server Operators
Change the system time	Modify the time setting of the system's internal clock	Administrators Power Users Server Operators
Force shutdown from a remote system	Shut down a remote server (not implemented)	Administrators Power Users Server Operators
Load and unload device drivers	Dynamically load and unload device drivers	Administrators
Log on locally	Log in to the system interactively	Account Operators, Admins . Backup Operators, Print Operators, Server Operators Everyone (on workstations)
Manage auditing and security log	Specify which objects are to be audited when auditing is enabled (which must be done by an administrator)	Administrators
Restore files and directories	Access or modify any file or directory on the system, regardless of its ACL	Administrators Backup Operators
Shut down the system	Shut down the local system (when logged-in interactively)	Administrators Server Operators Everyone (on workstations)
Take ownership of files or other objects	Assume ownership of files, directories, and other file-system objects, regardless of their access permissions	Administrators

Figure 2 – Basic User Rights
Source: Essential Windows NT System Administration – Aeleen Frisch

User Right	If you have this right, Then you are able to...	Groups Holding by default
Advanced User Rights		
Act as part of the operating system	Execute with operating system-level system access	None
Bypass traverse checking	Ignore directory permissions when accessing a file by full pathname	Everyone
Create a pagefile	Create and modify paging files	Administrators
Create a token object	Create a token object	None
Create permanent shared objects	Create shared operating system-level objects (not filesystem shares)	None
Debug programs	Execute with certain system debug bits set	Administrators
Generate security audits	Generate security audits	None
Increase quotas	Modify resource quotas (not implemented)	Administrators
Increase scheduling priority	Modify a process's execution priority upward	Administrators Power Users
Lock pages in memory	Force memory pages to re-main resident in real memory	None
Log on as a batch job	Register with the system as a batch job (designed for applications)	None
Log on as a service	Register with the system as a service (designed for applications)	None
Modify firmware environ-ment values	Change firmware parameter Values (hardware-dependant)	Administrators
Profile single process	Measure performance data for a single process (not implemented)	Administrators Power Users
Profile system performance	Measure performance data systemwide	Administrators
Replace a process-level token	Adjust aspects of a process's environment	None

Figure 3 – Advanced User Rights
Source: Essential Windows NT System Administration – Aeleen Frisch

Auditing File Access

For the purposes of this paper, the only audit class chosen in the Audit Policy is the success and failure of File and Object Access. This is not a recommendation for an appropriate audit policy for any existent or non-existent system but merely to fully demonstrate File Access auditing as a case study for the reader. Selecting the success and failure options will demonstrate the proper procedures for auditing access to these items and will assist in the demonstration of archiving baseline information or user trends.

From the Start Menu Select Administrative Tools ê User Manager for Domains. At the "Policies" menu select "Audit". Place a checkmark in the "Success" column and in the "Failure" column next to "File and Object Access". Note that auditing is only enabled at this screen but does not begin until files, folders, and/or printers are defined in each of their respective properties.

Keep in mind, in order to audit security events, it is necessary to have administrative privileges. When administering domains, the Audit Policy applies to the security policy of both the primary domain controller and the backup domain controller because they use the same Audit Policy.

File System Configuration

It is not possible to audit files or folders on a File Allocation Table (FAT) formatted volume. In order to successfully audit file access the drive containing the files to be audited should be formatted with Windows NT File System (NTFS).

Determining Volume Format

1. Double Click the "My Computer" icon from the desktop.
2. Right click the disk that contains the information to be audited and select properties.
3. Determine if the drive is NTFS or FAT [Fig. 4]

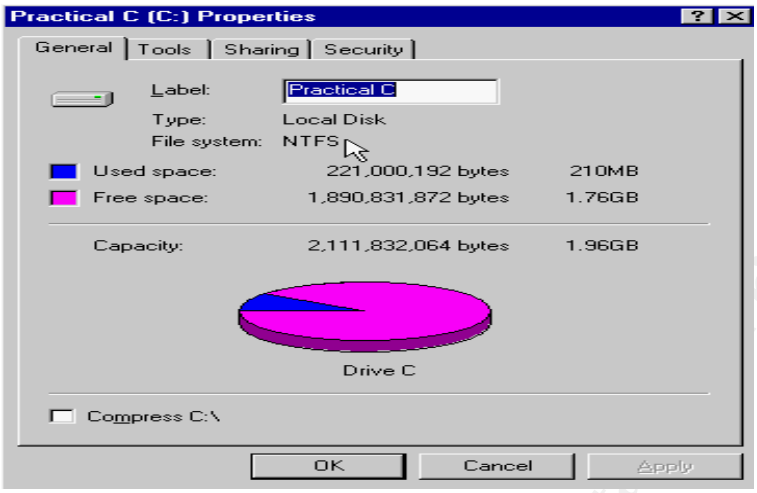

Figure 4 – Drive Properties

Converting FAT Formatted Volume to NTFS

1. From the start menu select Accessories ê MSDOS.
2. At the command prompt type convert c: fs : ntfs (use /v for verbose mode) [Fig. 5]
3. Restart the machine.

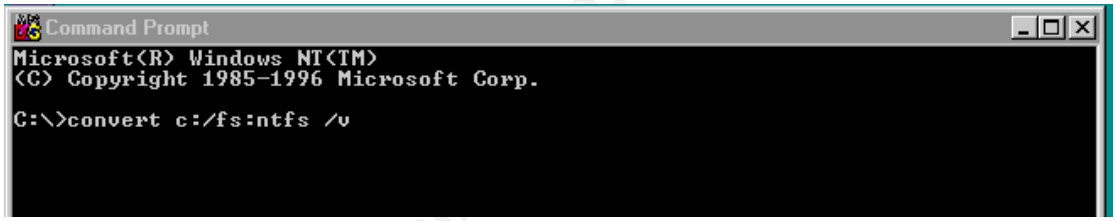

Figure 5 – Converting Disk from FAT to NTFS

Enable the System for File Auditing

1. From the Start Menu select Administrative Tools ê User Manager for domains.
2. From the Policies Menu select "Audit".
3. Place a checkmark in both the Success and the Failure boxes next to File and Object Access [Fig. 6].

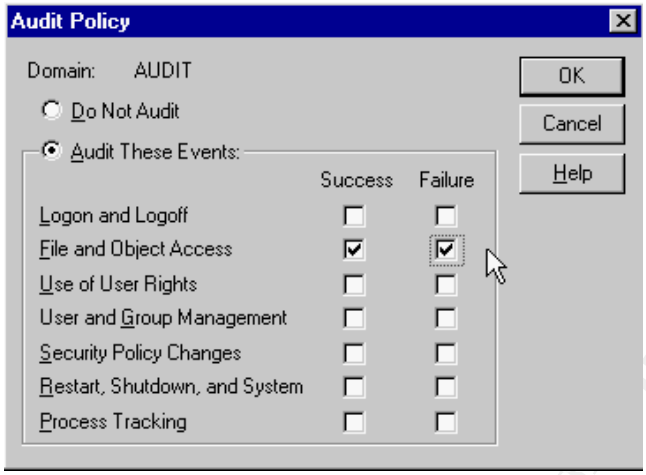

Figure 6 – Audit Policy w/ File and Object Access (Success and Failure).

4. Click "OK" when finished.

Setup of Auditing on Files and/or Directories

1. Start Windows NT Explorer
2. Right click the file or directory to be audited and select "Properties".
3. Select the Security Tab [Fig. 7].

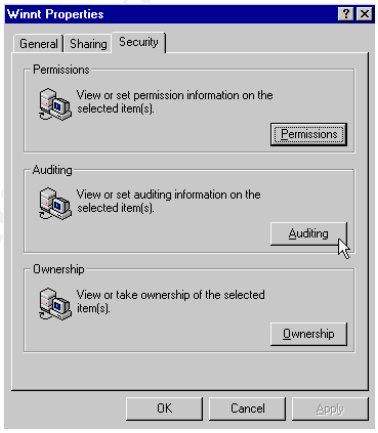

Figure 7 – Winnt Directory Properties Security Tab

4. Click "Auditing". Depending on the selection, a File Auditing or a Directory Auditing dialog box will appear.

   Auditing changes only apply to the directory and its files, subdirectories are not included. In order to include subdirectories, place a checkmark in the box next to "Replace Auditing on Subdirectories". If necessary, to apply changes to the directory only, place a checkmark in the box next to "Replace Auditing on Existing Files" [Fig. 8].

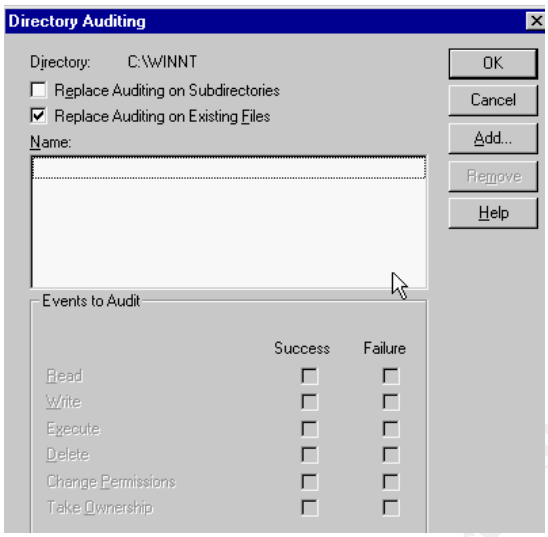

Figure 8 – Replace Auditing on Existing Files

Notice the "Events to Audit" Section is shaded out. Events cannot be selected until users/groups/domains have been chosen.

5. Click "Add". The Add Users and Group dialog box appears [Fig. 9].

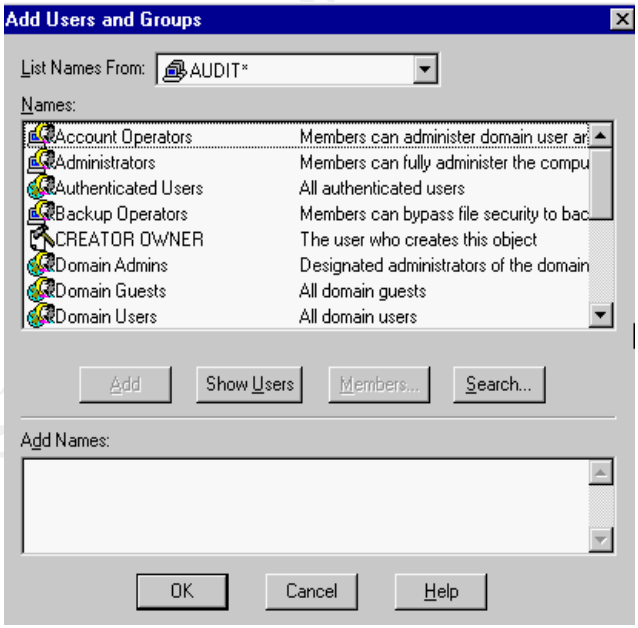

Figure 9 – Add Users and Groups to auditing.

6. Select the appropriate domain, users, and groups and click "Add" then click "OK".
7. Under Events to Audit [Fig. 10], click the success and failures boxes of the events to be audited.

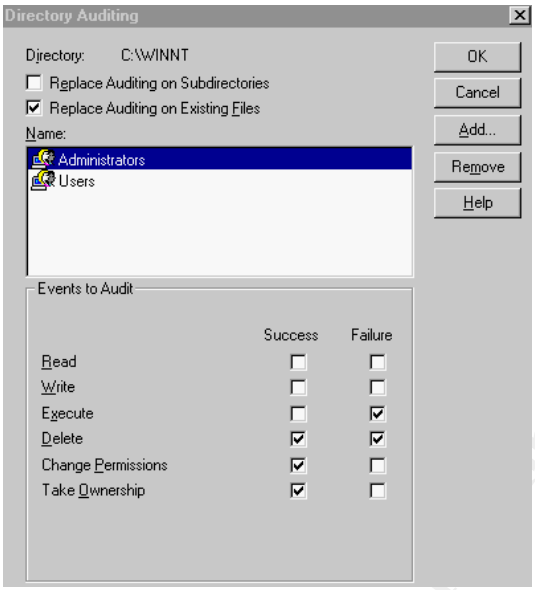

Figure 10 – Events Success/Failure Selection

8. Click "OK" to return to the Properties dialog box.
9. Click "OK" again – Auditing has just been set up for the directory/user/group/ selected in the steps above.

Removing File and Directory Auditing

1. To remove file or directory auditing for a user or group, just select the user or group and then click "Remove".

Using the Event Viewer

Windows NT System events, including errors, access violations, routine status messages, and auditing, are stored in three log files:

The System Log – Includes system error messages, and status messages for system reboots and other events. If system events are selected for auditing, these are also included in this log.

The Security Log – Includes messages relating to security. Security problems, such as incorrect logons, are included in this log if auditing is enabled. Security auditing is disabled by default.

The Application Log – Includes events logged by applications and problems such as application crashes.

To use the Event Viewer utility, from the Start menu select Programs ê Administrative Tools ê Event Viewer. This will display information from each of the log files listed above. Use the Log menu to select the file being displayed. It is possible to change the order for viewing events or search for events matching specific criteria.

Security Log Settings

Auditing File and Object Access can quickly result in the Windows NT Security logs becoming full. When the logs become full the system is no longer able to record events. This problem can be avoided by changing the settings of the Event Log.

One way to avoid the log filling up is by customizing the size of the security log in the Event Viewer. These logs can range from 64K in size to 4,194,240 K in size in increments of 64K. Default is 512K.

This problem can also be avoided by selecting one of the following three options: Overwrite Events as Needed, Overwrite Events Older than x Days, or Do Not Overwrite Events. CrashonAuditFail makes it possible to halt the system when the security log is full.

> Overwrite Events as Needed – by selecting this option the system will always overwrite the oldest events with the most recent. This could be used on a low maintenance system. Keep in mind, however, that it is also very easy to for a hacker to overwrite these events to flush out log files with meaningless entries.
>
> Overwrite Events Older than x Days – Allows an administrator to determine the number of days to retain in the event log. The default is seven. This is a good choice (maybe the best) if you are archiving the logs regularly. Be sure that the log does not fill up at a rate that exceeds the archive schedule.
>
> Do Not Overwrite Events – Requires the log to be cleared manually. This is a good choice when the administrator cannot afford to miss any events (usually a high security system). It can also be used in conjunction with the CrashOnAuditFail registry setting.
>
> CrashOnAuditFail – Is a good choice for security. It requires administrator intervention when the log fills up. This is good for catching hackers trying to flush the system. However, this option also has a downside: it can be used as a denial of service attack on a system that is required to be operational the majority of the time (such as a web store interface).

To halt the system when the security log fills, you must create or assign the following registry key with a Registry Editor such as regedit.exe or regedt32.exe. Remember changes will only take effect after the system is restarted. Update the Emergency Repair Disk after changes have been made.

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	\CurrentContolSet\Control\Lsa
Name:	CrashOnAuditFail
Type:	REG_DWORD
Value:	1

Once the system is halted as a result of the registry key above, the system must be restarted and reconfigured in order to halt the system again when the security log fills up. Remember only system administrators can log on to the system until the security log is cleared.

Securing the Event Log Files

The volume that contains the folder \%SystemRoot%\System32\Config should be formatted with NTFS. In this folder there are three event logs SysEvent.evt (the System Log), SecEvent.evt (the Secuity Log), and AppEvent.evt (the Application Log), which are viewable in the Event Viewer. Use NTFS permissions to control access to these files. The Administrators group along with the System account should be granted full control of these files [Fig. 11]. All other access should be assigned on a case-by-case basis. In addition to assigning NTFS permissions, NTFS auditing should also be enabled to these files. Administrators should be audited for successes and failures, the "Everyone" group should be audited for failures in all categories, and the system account should not be audited [Fig. 12]

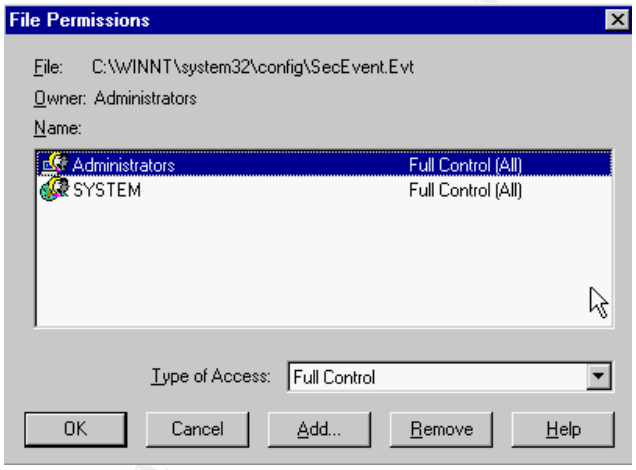

Figure 11 – Granting File Permissions to the Event Logs limited to Administrators & System

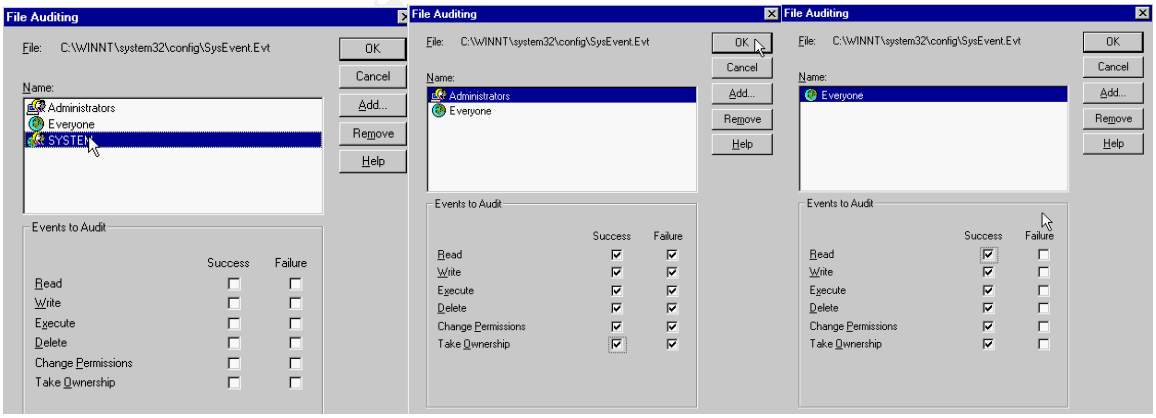

Figure 12 - Auditing Event Logs - Everyone/Administrator/System Settings

In User Manager there is a user right named "Manage Auditing and Security Log". This right should only be assigned to select individuals within the Administrators group.

Viewing the Security Log

From the Start menu select Programs ê Administrative Tools ê Event Viewer. From the log menu, click Security [Fig. 13].

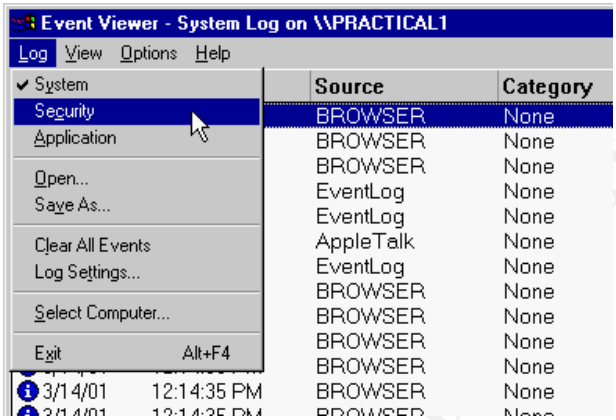

Figure 13 – Selecting the Security Log in Event Viewer.

Most event logs consist of a header, a description of the event (based on the event type) and a description. Event Viewer displays events from each log separately. Each line shows information about one event. This information includes the type, date, time, source, category, event ID, user account, and computer name. The type header of a security log records "Success" audit events or "Failure" audit events. In the Event Viewer's normal list, events are represented by a key (Success) or a lock (Failure). The "Date" header contains the date the event took place. The "Time" header contains the local time of the event. The "Source" header provides information on the software that logged the event, which can be an application name, a component of the system, or a component of a large application, such as a driver name. The "Category" header indicates the classification of event by the event source. This information is primarily used in the security log. For security audits, this corresponds to one of the event types for which success or failure auditing can be enabled in the User Manager Audit Policy. The "Event ID" header provides a number, which identifies the particular event type. This information can be used by support representatives to troubleshoot system problems. The "User" header logs information on whose behalf the event occurred. This name is the client ID if the event was actually caused by a server process or the primary ID if impersonation is not taking place. Where applicable, a security log entry contains both the primary and impersonation IDs. The "Computer" header logs information about where the event took place. To view detailed information for any event, select the event and then on the View menu, click "Detail" or double click the event and it will automatically open the "Event Detail" window [Fig. 14].

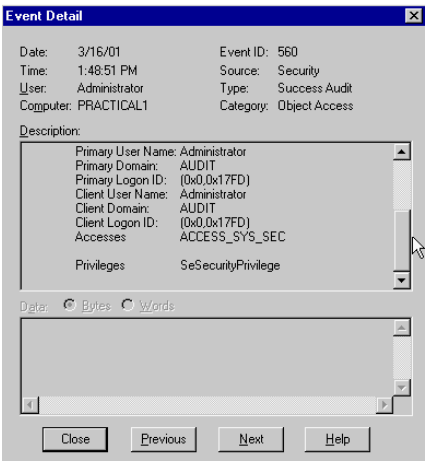

Figure 14: Event Detail Window

Filtering and Finding Security Log Events

When starting the Event Viewer, all the events recorded in the log appear automatically. It is possible to change the appearance of the log, to display specific events, by using the "Filter Events" command and the "Find" command.

Finding or Filtering Events

1. Start "Event Viewer"
2. Select "Filter Events"[Fig. 15] or "Find" [Fig. 16] from the View menu.
3. Select appropriate criteria [Fig. 17].

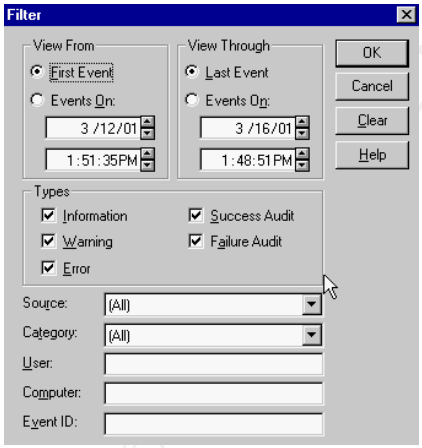

Figure 15 – Filter Event Window

Figure 16 – Find Event Window

4. Click OK.

Filter and/or Find Criteria

Filter Options	Description
View From / View Through	Filter only: Specify the dates for which you wish to view events.
Types	Select the types of events that you want to view. (Success or Failure.)
Source	Specify the software or component driver that logged theevent.
Category	Select the classification of the event as defined by thesource.
User	Specify a user account to locate events resulting from a specific user.
Computer	Specify a computer name to locate events resulting from a specific computer.
Event ID	Shows an event number to identify the event.
Description	Find option only: Specify text that would appear in the description of the event.

Figure 17 – Filter and/or Find Criteria
Source: Microsoft Official Curriculum Administering Microsoft Windows NT 4.0

Archiving the Security Log

The Windows NT resource kit provides the following fundamental description on Archiving the Security Log:

> In Windows NT, when archiving an event log, it can be saved it in one of the following formats:
>
> 1. Log file format, enables the archived log to be viewed again in Event Viewer.
> 2. Text file format, enables use of the logged information in an application such as a word processor.
> 3. Comma-delimited text file format, enables use of the logged information in an application such as a spreadsheet or a flat-file database.
>
> Binary event data is saved if the log is saved in log file format, but is lost if saved in the other two (text file format, or comma-delimited text file format). Event descriptions are saved in all archived logs. When archiving a sorted log, the sort order affects the order in which event records are archived in a text file format or comma-delimited file format. However, sort order does not affect the order of

event records in a log archived in log file format. The sequence of data within each individual record is saved in the following order: Date, Time, Source, Type, Category, Event, User, Computer, and Description. Archiving the log has no effect on the current contents of the active log. To clear the original log, select "Clear all Events" from the Log menu. To remove an archived file, delete the file by right clicking and choosing "Delete" or simply drag the file to the recycle bin.

Saving Security Log File for Archival

1. From the Start menu select Programs ê Administrative Tools ê Event Viewer.
2. From the Log menu select "Save As".
3. Select a location for the file and type a file name.
4. Select the format to save it in (log file format, text file format, comma-delimited text file format) [Fig. 18].

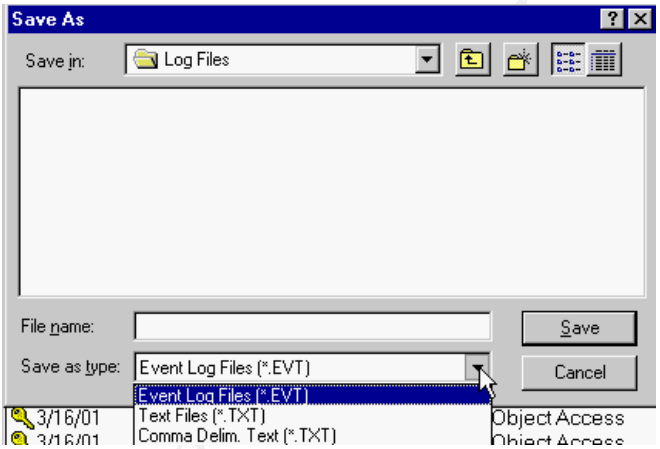

Figure 18 – Selecting Log File Format

5. Click the "Save" button.

Clearing the Security Log

1. From the Start menu select Programs ê Administrative Tools ê Event Viewer.
2. From the Log menu select "Clear All Events".
3. The system will prompt to save the log before clearing it. Select the appropriate answer [Fig. 19].

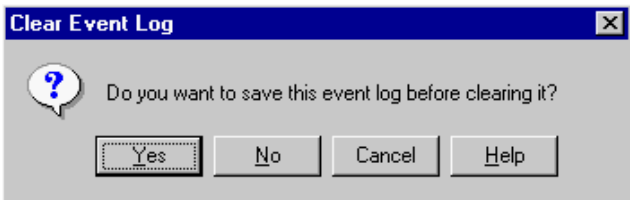

Figure 19 – Saving the Event Log before clearing.

4. If "No" is selected, the system will warn that the action being taken is irreversible, [Fig. 20].

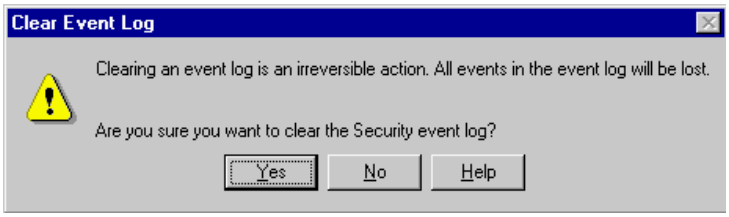

Figure 20 – Clear Event Log without saving warning.

5. The security log will create an entry stating that the log has been cleared [Fig. 21].

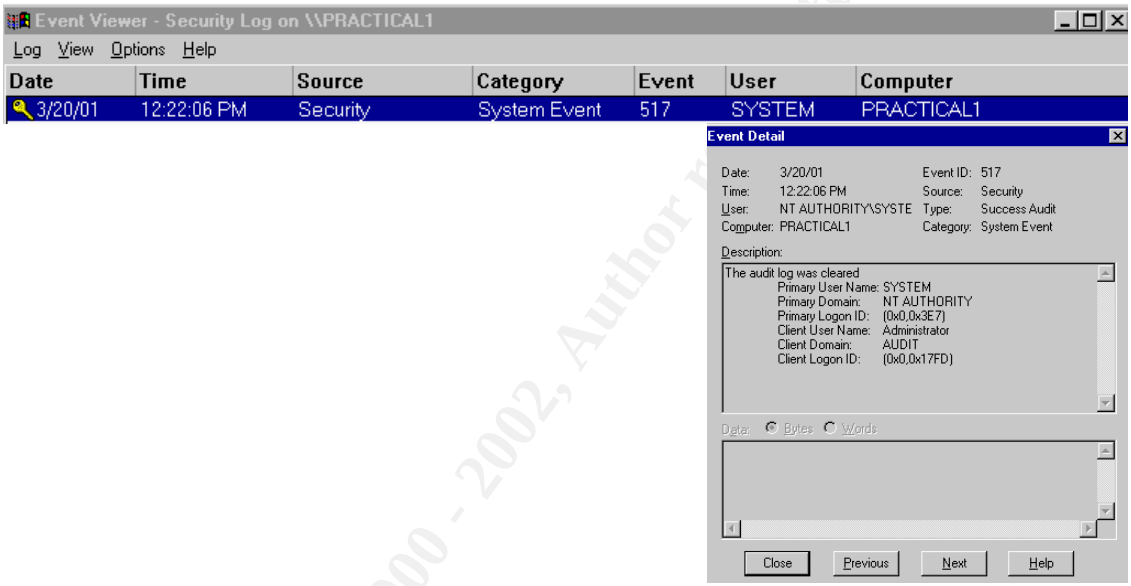

Figure 21 - Security Log Event: Audit Log was cleared.

Viewing an Archived Security Log Saved in Log File Format– Step by Step

1. From the Start menu select Programs ê Administrative Tools ê Event Viewer.
2. From the Log menu select "Open…"and select the path and name of the file to be opened [Fig. 22].

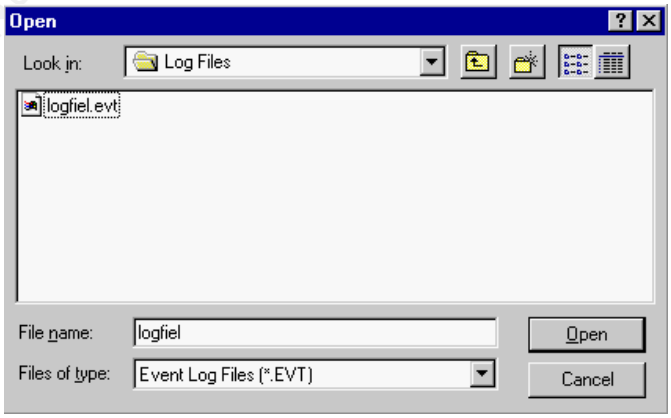

Figure 22 – Opening Security Log Saved in Log File Format.

3. Click “Open”.
4. An “Open File Type” window appears. Select the radio button next to security [Fig. 23].

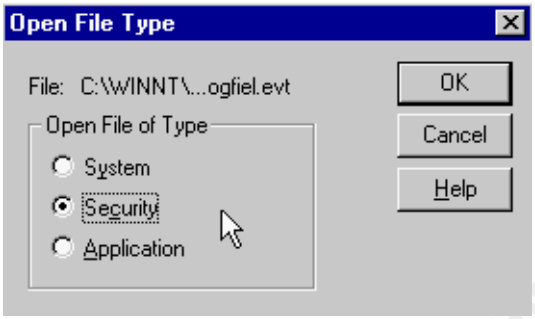

Figure 23 – Open File Type…Security

5. Click “OK”.
6. The file will be opened in the Event Viewer log file. It is still possible at this point to use the find option and the filter event option (See figures 15 and 16).

Viewing an Archived Security Log Saved in Text File Format– Step by Step

1. Open a word processor (WordPad, Notepad, Microsoft Word, Word Perfect, etc.).
2. From the File menu of the word processor select “Open…” and select the path and name of the file to be opened.
3. Click “OK”.
4. The file will be opened in text format [Fig. 24]. At this point it is no longer possible to use the find option and filter event option.

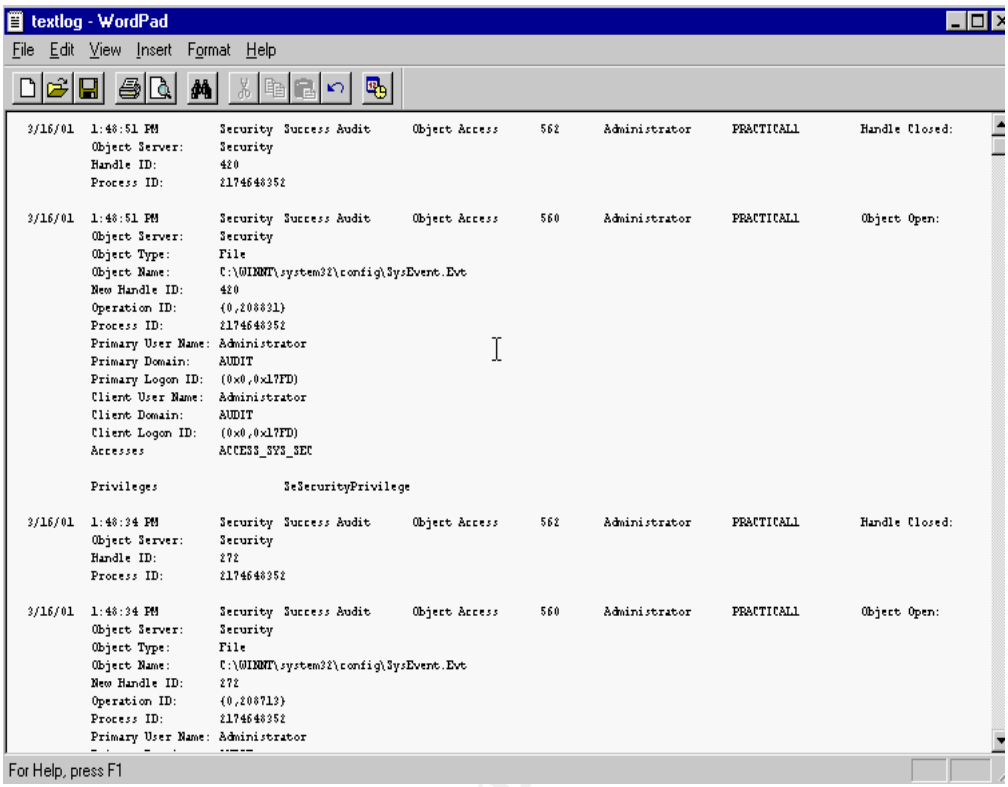

Figure 24 – Security Log in Text File Format as viewed in WordPad.

Recommendation: Save two copies of the security log. One copy in event format and one copy in comma-delimited text file format for detailed review at a later date.

Testing - Auditing of Files and/or Folders

Testing the audit policy that has been established will assist the system administrator in determining if the policy was setup correctly. It is recommended that each file be tested that is considered proprietary or sensitive to an organization to make sure access attempts are being denied to those users without the authority to view the document. It is also a good way of double checking the Windows NT security settings to be sure they have been set up appropriately. In order to illustrate the testing of the audit policy established, the administrator account will be used to "Take Ownership" of a file in the \winnt directory (see figure 10)

1. Log in using the Administrator account.
2. From the Start menu select Programs ê Administrative Tools ê Event Viewer.
3. From the Log menu, select "Security"[Fig. 25].

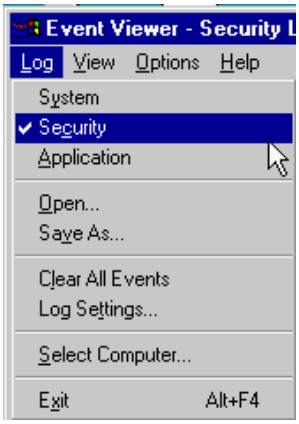

Figure 25 – Event View Log Selection – Security

4. Again, from the Log menu, select "Clear All Events" [Fig. 26].

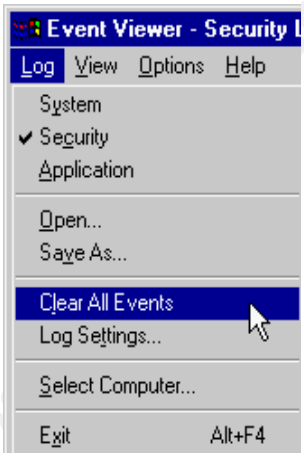

Figure 26 – Event View Log – Clear All Events

5. At the Clear Event Log window, respond to "Do you want to save this event log before closing" [Fig. 27] by selecting "No".

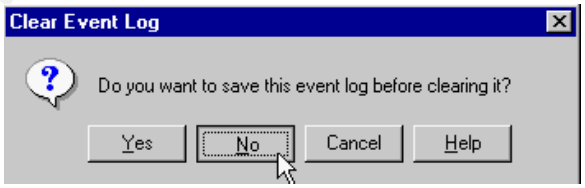

Figure 27 – Clear Event Log window

6. At the Clear Event Log Warning window [Fig. 28], the system will warn, "Are you sure you want to clear the Security event log?" select Yes.

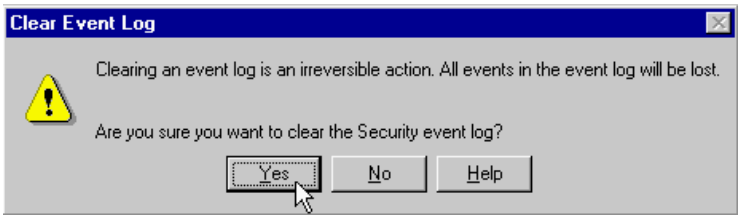

Figure 28 – Clear Event Log Warning Window

7. Leave Event view open.
8. From the Desktop right-click the "My Computer" icon.
9. Select "Explore".
10. Double click the volume of the file chosen for audit.
11. Right click the file chosen for audit. (In this case, any file or folder in the \winnt directory will do).
12. Select "Properties" and select the "Security" tab [Fig. 29].

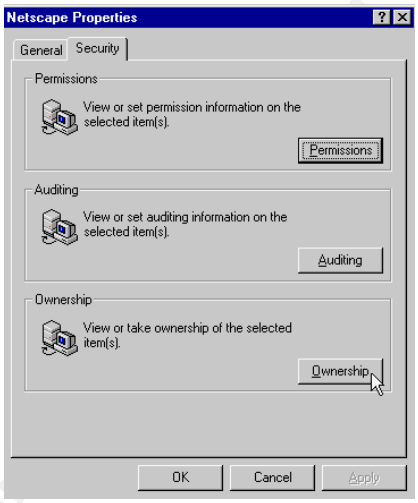

Figure 29 – Properties window/security tab.

13. Click on " Ownership".
14. In the "Owner" window click "Take Ownership" [Fig. 30].

Figure 30 – Owner Window/Take Ownership

15. Click "OK" at the Properties window.
16. Return to "Event Viewer".
17. From the View menu select "Refresh" [Fig. 31].

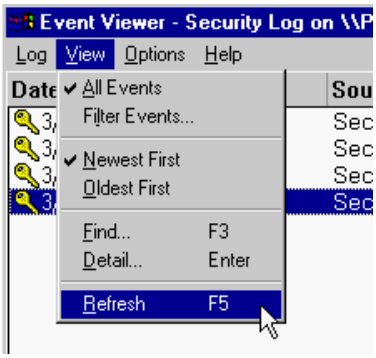

Figure 31 – Refresh the Security Event Log

18. From the View Menu select "Find". In the Description box type "ownership" [Fig. 32].

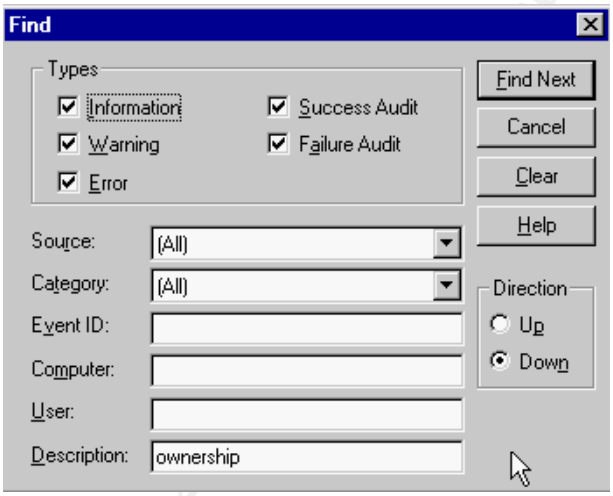

Figure 32 – Find Events that contain "ownership"

19. Select "Find Next".
20. Double click the event selected.
21. Scroll to the bottom of the Description window to confirm that the event Privileges reads "SeTakeOwnershipPrivilege" [Fig. 33].

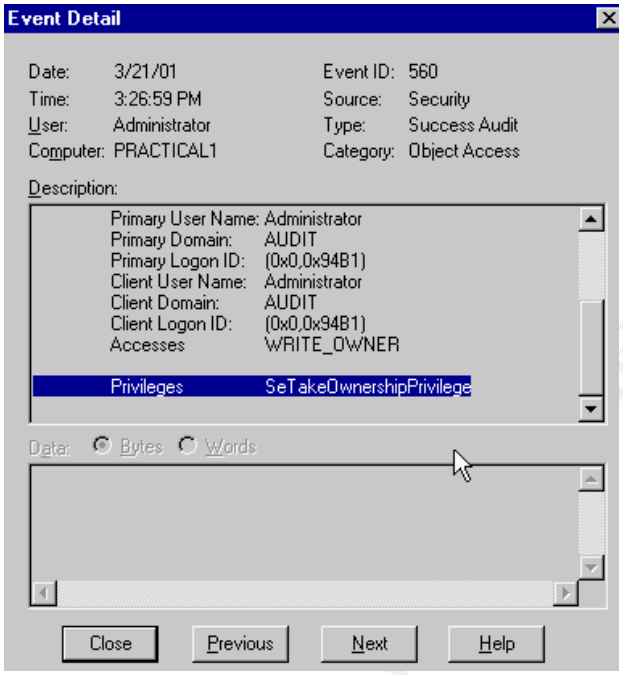

Figure 33 – Event Detail Description – Privileges: Take Ownership

22. Select "Close" on the Event Detail Window.
23. Close the event Log.

The auditing of "Take Ownership" by the Administrators group has been confirmed. If there are questions about the implementation of an audit policy, each audit event should be tested prior to deployment of the computer systems.

Establish A Review Policy

With security auditing enabled, it is possible to identify the normal use of a system and detect when a breech in security is attempted or has been accomplished. However, even though security auditing has been enabled, a policy should be in place to review the log files on a regular basis. A lack of reviewing the security logs renders the auditing controls ineffective. It is recommended that the security audit logs be reviewed on a weekly basis at a minimum and, as often as daily, depending on a company's security environment. A review policy should include a detailed list of each security event audited, the name of the person responsible, the date and time completed, a comment section for security anomalies. It should also include evidence of administrator review and a signature or initial section to establish who completed the review [Fig. 34]. This review sheet should be kept in a locked drawer only accessible to system administrators so potential intruders can not determine what features are being audited.

Security Log Audit Review Sheet

Event Log Checed for	Anomolies Found	Action Taken	Date	Time	Signature
Logon/Logoff - Success					
Logon/Logoff - Failure					
File and Object Access -Failure					
Use of User Rights - Failure					
Security Policy Changes - Success					
Security Policy Changes - Failure					
Restart, Shutdown, and System -Success					
Restart, Shutdown, and System - Failure					

Event Log Checed for	Anomolies Found	Action Taken	Date	Time	Signature
Logon/Logoff - Success					
Logon/Logoff - Failure					
File and Object Access -Failure					
Use of User Rights - Failure					
Security Policy Changes - Success					
Security Policy Changes - Failure					
Restart, Shutdown, and System -Success					
Restart, Shutdown, and System - Failure					

Event Log Checed for	Anomolies Found	Action Taken	Date	Time	Signature
Logon/Logoff - Success					
Logon/Logoff - Failure					
File and Object Access -Failure					
Use of User Rights - Failure					
Security Policy Changes - Success					
Security Policy Changes - Failure					
Restart, Shutdown, and System -Success					
Restart, Shutdown, and System - Failure					

Event Log Checed for	Anomolies Found	Action Taken	Date	Time	Signature
Logon/Logoff - Success					
Logon/Logoff - Failure					
File and Object Access -Failure					
Use of User Rights - Failure					
Security Policy Changes - Success					
Security Policy Changes - Failure					
Restart, Shutdown, and System -Success					
Restart, Shutdown, and System - Failure					

Event Log Checed for	Anomolies Found	Action Taken	Date	Time	Signature
Logon/Logoff - Success					
Logon/Logoff - Failure					
File and Object Access -Failure					
Use of User Rights - Failure					
Security Policy Changes - Success					
Security Policy Changes - Failure					
Restart, Shutdown, and System -Success					
Restart, Shutdown, and System - Failure					

Figure 34 – Security Log Audit Review Sheet

Conclusion

Microsoft Windows NT provides valuable, easy to implement file-auditing tools, which will yield valuable security data provided you actually review it. This data is an important weapon against the ever-present hacker threat. By assuring the integrity and validity of the data, files, and system itself, file auditing can be as important as a system or data backup. Auditing File and Object Access is just one small part of the many auditing tools available with Windows NT without the use of third-party products. There are many other security features that can be implemented to ensure the integrity of any Windows NT system. Once an organization has determined the appropriate balance of security and functionality for their systems, they do not need to look much further, than to the system itself, to find simple easy-to-use security enhancements that will tighten security on their system and make their administrative experience much more successful.

References

Microsoft Press, Microsoft Windows NT Resource Kit, Microsoft Press 1996.

Frisch, Æleen, Essential Windows NT System Administration, O'Reilly & Associates, Inc. 1998

Fossen, Jason, Securing Windows NT, Step-by-Step, The SANS Institute 2000

Michael, Moncur, MCSE The Core Exams in a Nutshell A Desktop Quick Reference, O'Reilly & Associates, Inc. 1998

Microsoft Official Curriculum, Administering Microsoft Windows NT 4.0, Microsoft Corporation 1999

Goncalves, Marcus, Windows NT 4.0 Server Security Guide, Prentice Hall 1998

The SANS Institute, Windows NT Security Step by Step Version 2.1.5, The SANS Institute, 1999

Heckerdorn, Sherri, GIAC Certification in NT Security, http://www.sans.org/y2k/practical/Sherri_Heckerdorn.doc

Last Updated: September 22nd, 2017

Upcoming Training

Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
Southern California- Anaheim 2018 - SEC505: Securing Windows and PowerShell Automation	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**vLive**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**