Global Information Assurance Certification Paper

Issues with Auditing Window NT 4.0 Server

by

Michael J. Moore

GIAC NT

Practical Assignment for Capitol SANS 2000
Securing Windows
Washington, DC
December 2000

TABLE OF CONTENTS

Introduction/Objective

This paper was written to fulfill requirements for the SANS Level Two, Securing Windows, GIAC NT Practical Assignment. The information contained herein is intended to demonstrate knowledge of the auditing capabilities of Windows NT Server 4.0. There is no intent to suggest a definitive audit policy for any organization. Nor is the intent to endorse any particular practice or use of any tool mentioned in this document.

As part of my preparation and research for this endeavor, I reviewed the practical assignments completed by other SANS students which pertain to Windows NT auditing and are currently posted on the SANS web site. Many of the assignments currently posted provide quality and informative data on how auditing is enabled, suggestions for what to audit, suggestions for dealing with Event Viewer logs, ideas to further secure a Windows NT Server installation and other information beneficial to the security-minded computing community.

In order to demonstrate my knowledge of auditing it is necessary to rehash some of what has already been discussed in other students' practical assignments. However, my experience with Windows NT 4.0 Server and specifically auditing issues, will, I believe, allow me to present new and interesting subject matter and make some observations concerning auditing that have not yet been addressed in other practical assignments. It is my hope that this information is not only informative but also practical and helpful for those who are involved with issues related to Windows NT auditing.

Not every company, agency or business has the funding to support the most desirable, latest and greatest tools, services, or technologies available for securing and auditing its computing infrastructure. For example, I have been associated with individuals whose job it is to go out to a site to retrieve and save Windows NT logs to be examined at a later time and different location from where the logs were retrieved. Unfortunately, those individuals indicated that they did not have an NT machine at the viewing location on which to examine the saved logs! As unbelievable as this may sound, I assure you this is the reality of some unfortunate circumstances. This being the case, I have taken resource limitations into consideration as I prepared this assignment.

Most of what I address within this document will pertain to a default installation of Windows NT Server 4.0 and subsequent utilization of functions, tools, and commands that come bundled with the operating system or are freely available on the net. Service Pack 4 has been installed on all systems used for demonstration and all systems are configured with the NTFS file system. For demonstration purposes, screenshots will be taken from a PDC of a single domain or an NT Workstation. The only client computers I address are NT Workstations.

James D. Murray describes auditing as, "the policy and procedure of monitoring, recording, and receiving both system and user activity: the history of security events is called the *audit trail*, which is stored in the a*udit log*. The most commonly audited events

are those related to system, user, and network activity."[1] This being said, unfortunately, there is no magic formula for calculating exactly what system, user, and network activity should be audited for any given situation or environment. There are many suggestions provided by many different sources. My point here is not to proffer a best practice policy that might be appropriate for a particular environment equipped with particular resources. My point is that you first must decide and then enable auditing. By default, auditing is not enabled on a fresh installation of a Windows NT Server 4.0.

Assume that an audit policy has been established and it has been determined exactly what information will hopefully be captured. Further assume that the Administrator has put forth a diligent effort to ensure that auditing has been enabled to collect the desired information. Could you imagine the Administrator's horror when he or she opens the Event Viewer Application only to find that the logs do not contain any information pertaining to actions that took place and were thought to be under audit? Not only could this be disheartening and embarrassing, it could cost an Administrator his or her position.

In the course of my experience with Windows NT Server and auditing, I have come across situations like the one described above. No matter how experienced, Administrators, like anyone else, are prone to mistakes. These mistakes can be costly in terms of the loss of the ability to identify malicious activity or unauthorized attempts to access resources on your systems.

As mentioned previously, this document will revisit much of what my fellow SANS students have already written. However, I will also point out some of the more common mistakes that I have come across when attempting to enable auditing, as well as offer a few suggestions in reference to the NT Event Viewer logs. I will also make a few observations on looking for evidence of an attempted intrusion or misuse not only in logs but also in other places if your logs do not contain the desired entries.

Enabling Auditing on the System

As previously mentioned, there is no auditing enabled by default on a fresh installation of Windows NT Server 4.0. In order to enable auditing, open the Administrative Tool, User Manager for Domains. Select Policies on the toolbar and Audit in the drop-down menu. You should be presented with a screen similar to that in Figure 1.

[1] Murray, James D. *Windows NT Event Logging* (O'Reilly & Associates, 1998) page 7.

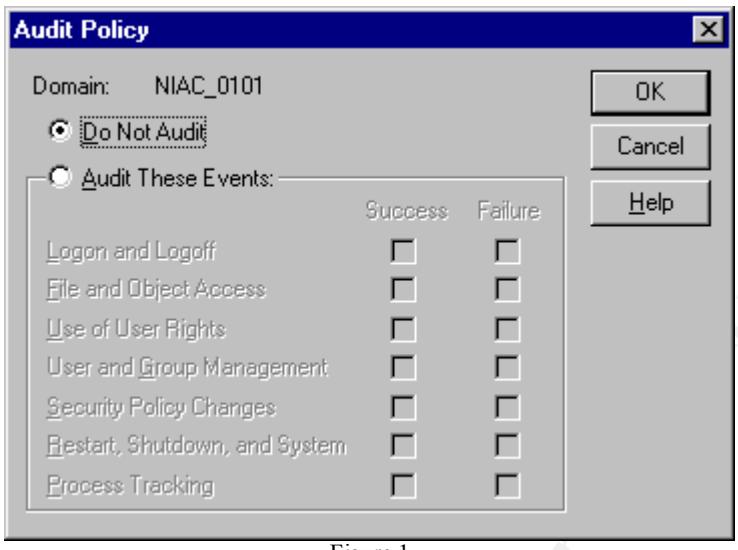


Figure 1

Until auditing is enabled in this location there will be no auditing events generated in the Security Log of Event Viewer.

Again, my purpose is not to propose that there is an ideal audit policy. However, I will note that the authors of *Windows NT Server 4 Security Handbook* recommend that, "you should (as a bare minimum) enable the features shown…"[2] They illustrate their recommendation with a screenshot similar to the one below in Figure 2 with the identical items enabled for auditing.

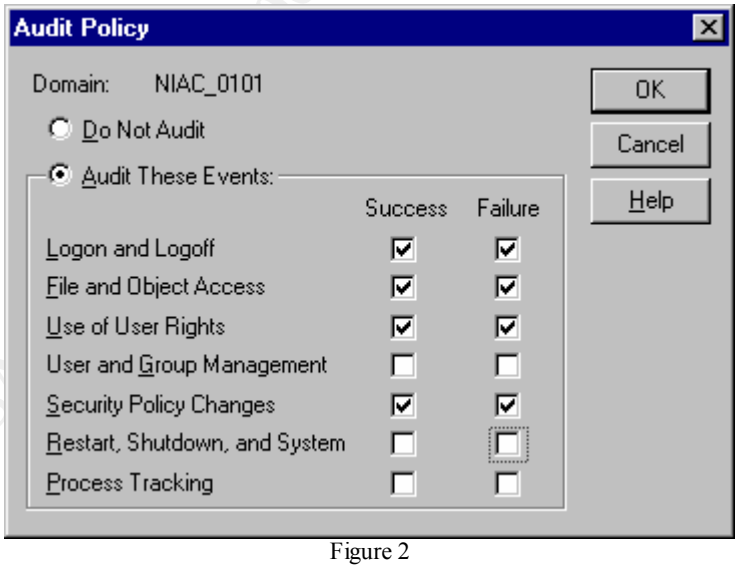


Figure 2

[2] Hadfield, Lee et al. *Windows NT Sever 4 Security Handbook* (Que® Corporation,1997) page 306.

In the book *Hacking Exposed*, referring to privilege escalation the authors state, "A similar approach is to plant booby traps on the system that get launched in conjunction with some regular system event (such at rebooting)."[3]

In his practical exercise, Steven Toy offers a suggestion for auditing in a "medium security" environment. Referring to Restart, Shutdown, and System he states, "In a high security situation you may want to know every time a system is shut down and restarted, but in the case of my medium security situation, I don't need to know this and it would just cause additional log entries."[4]

Since some exploits require the system to be restarted, I would consider it prudent to audit the Restart, Shutdown, and System option for at least Success regardless of the environment, high or medium security. The "additional log entries" caused by audit of these events would most likely be minimal but could be worth a fortune in the information they provide. I respect the opinions of both the authors of *Windows NT Server 4 Security Handbook* and Steven Toy, but I humbly submit that, at the least, Success for this event should be tracked.

There are numerous factors that will determine if not drive auditing policies for many organizations. Naturally, the sensitivity or value of the data stored on a system is a major contributing factor to developing policy. Realistically, however, the amount of support the Administrator receives from his or her management in terms of both resources and personnel may determine what events are ultimately chosen for audit. Auditing many events can degrade heavily used systems that are burdened by limited resources. Additionally, reviewing log files can be a long and tedious process. Depending on the number of users and events identified for audit, thousands of entries can easily be generated in the log files in a short period of time. Even with the filtering capabilities built into the Event Viewer Application, it could take a substantial amount of time to examine large log files with adequate scrutiny to identify items of concern. It is quite possible that additional personnel would be required to devote time to such an effort.

Confirming Auditing

In their practical assignments Martin A. Golias[5] and Christopher Carboni[6] demonstrate a step that all Administrators might consider making a routine part of their duties. In Section 3 of his document Mr. Golias first demonstrates how items are selected for auditing. He then, very wisely checks to verify that what he intended to select is actually what the system will audit. He actually pulled up the entry for the Audit Policy Change

---

[3] Scambray, Joel et al. *Hacking Exposed Second Edition Network Security Secrets & Solutions* (Osborne/McGraw Hill, 2001) page 172.

[4] Toy, Steven "Centralized Auditing of a Windows NT Computer" http://www.sans.org/y2k/practical/Steven_Toy.doc

[5] Golias, Martin A. http://www.sans.org/y2k/practical/Martin_Golias.doc

[6] Carboni, Christopher http://www.sans.org/y2k/practical/Chris_Carboni.doc

event in the Security Log to ensure system auditing was enabled properly. Mr. Carboni demonstrates the same technique on page 6 of his practical. In order to view the entry in the Security Log of Event Viewer, Success for Security Policy Changes would have to have been selected for auditing. I will illustrate just how useful it may be to verify audit configuration settings later in this document when I discuss enabling auditing on objects.

DumpSec, a tool freely available at http://www.somarsoft.com/, will also allow you to view and verify current audit policy for your system. (It is also very useful for other purposes). Download from the web and extract the .zip file. Execute DumpSec to view the window in Figure 3.

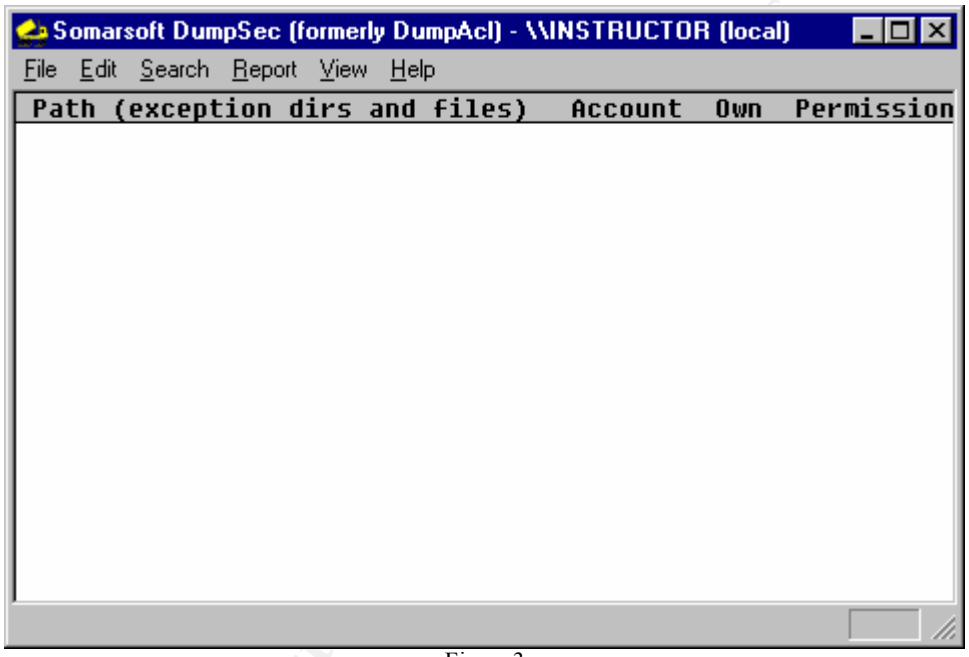


Figure 3

Click on Report on the toolbar as in Figure 4 and select Dump Policies near the end of the drop-down menu.

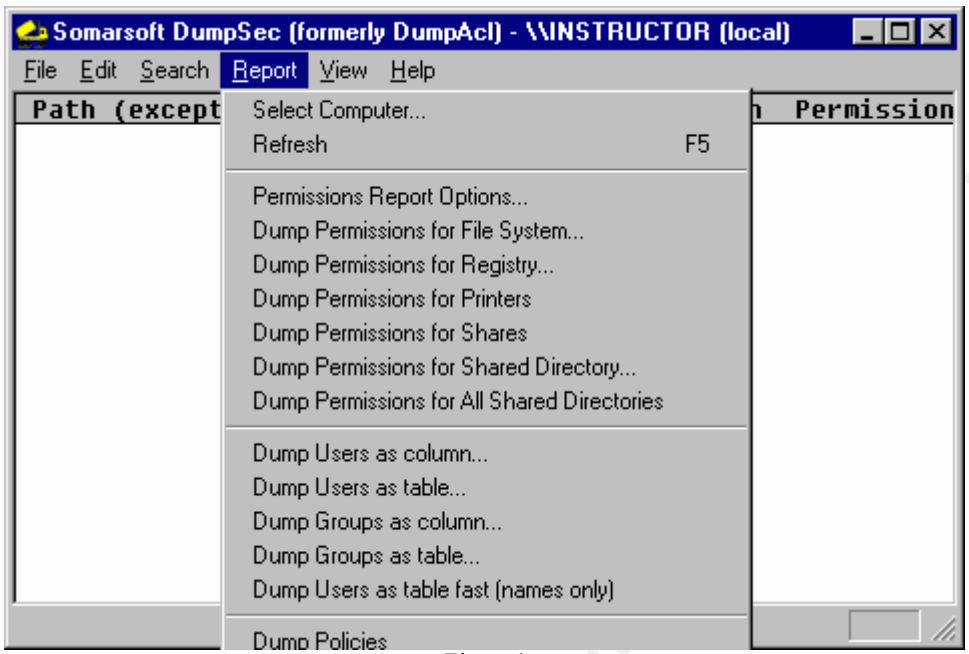


Figure 4

Figure 5 is an example of data compiled as a result of the Dump Policies option. Again, this is another way to verify that what is intended to be, is actually being audited on the system.

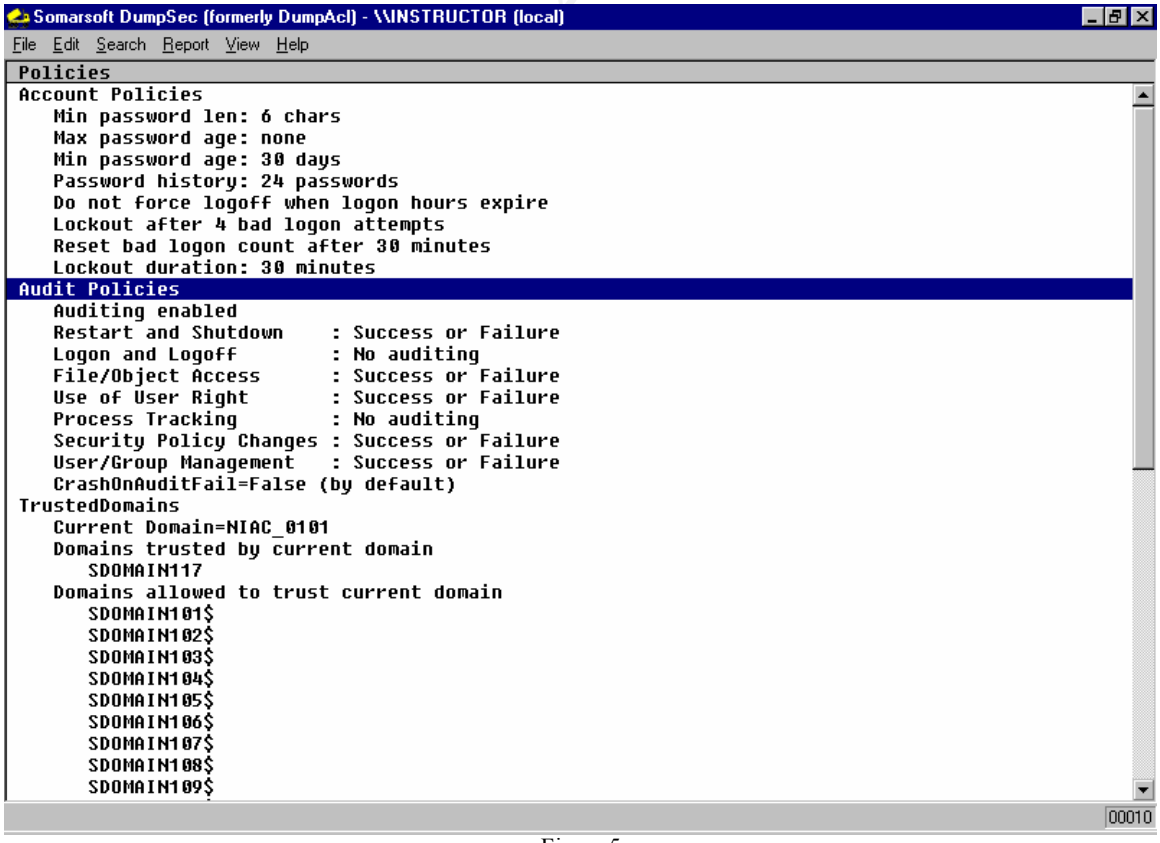


Figure 5

Much has been written about auditing the Windows NT system. Many SANS students have addressed the issue in depth in their practical assignments. However, the fact that File and Object Access has been enabled in User Manager for Domains does not mean that any events will be generated in the Security Log when a user attempts to access a particular object unless auditing has also been enabled on that object through its properties. I have not seen enabling auditing on objects discussed in depth in any other practical assignments. Brig Otis, in his practical assignment states, "You can instruct NT to audit in more detail via the Security Tab of the Properties dialog for files and folders."[7] Ruth Parish, in her practical assignment[8], provides an excellent example of why file and directory auditing is important for certain objects. However, there is no detailed description of enabling auditing on an object in either of these practical assignments. I will follow up on the practical assignments of Ms. Parish and Mr. Otis by demonstrating how to enable auditing on directory and file objects.

Not only is it essential to enable auditing on certain objects in order to track access, but most importantly, to be effective it must be enabled properly. Earlier in this document I mentioned that it might be wise for Administrators to consider making verification of audit configuration settings a routine part of their daily duties. Too often Administrators are rushed to accomplish even simple tasks. They quickly point and click with good intentions but can inadvertently make a simple oversight resulting in undesired results or loss of data.

In order to point out the importance of verifying settings, I will also address that issue and other concerns with a demonstration of enabling auditing on objects. For demonstration purposes I have chosen to use a folder on a development machine at my workplace. The folder is named "TopSecret" and contains 2 "secret" files.

Auditing a Folder Object

As previously indicated, in order to audit any object that will result in events being generated in the Security Log, the File and Object Access option has to be selected in the audit dialog box in User Manager for Domains. Once that is accomplished you can go to the properties of any object in Windows Explorer to enable auditing of that particular object. Figure 6 below, demonstrates how to access the desired object's properties from Windows Explorer. Once highlighted, right click on the object to display the drop-down menu. Select and open the properties.

[7] Otis, Brig, SANS Practical, Track 5: Windows Security Monterey, 2000 (page 25) http://www.sans.org/y2k/practical/brigs_otis GCNT.doc

[8] Parish, Ruth Anne "An In-Dept Examination of Event Viewer and Auditing" http://www.s1ans.org/y2k/practical/Ruth_Anne_Parish_GCNT.doc (page 11)

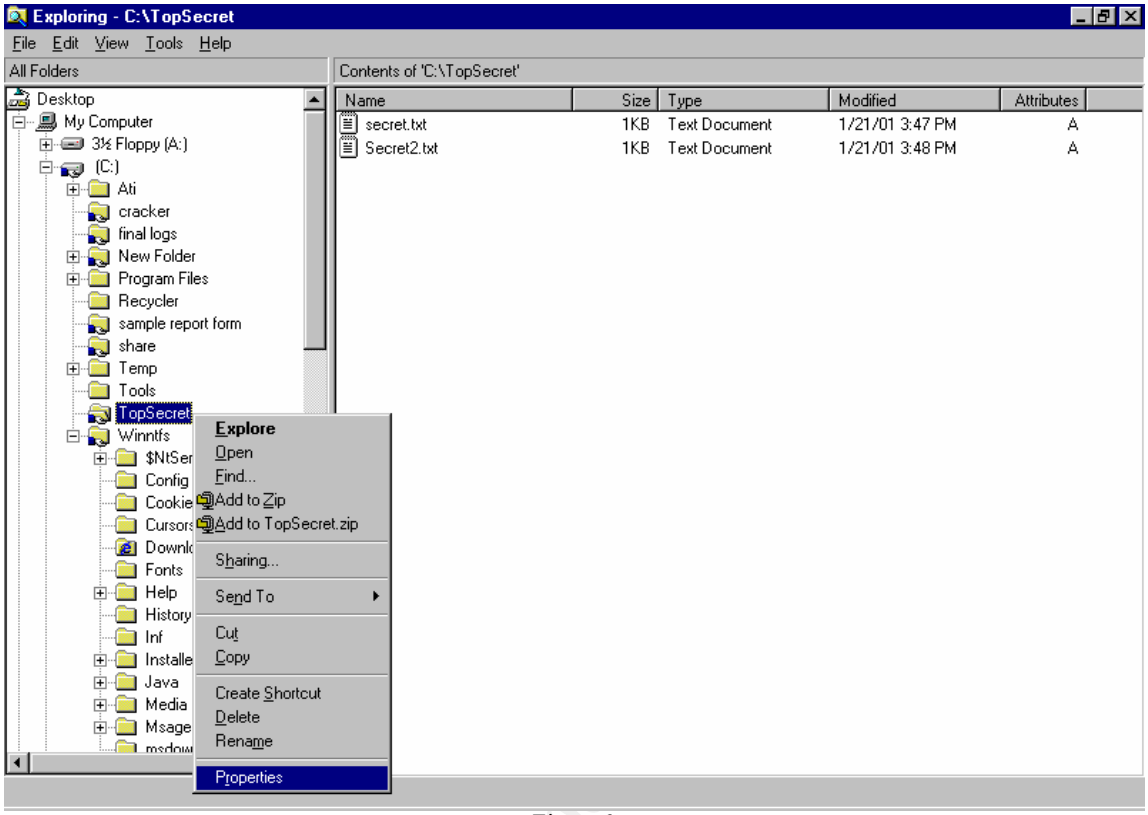


Figure 6

Figure 7 below, shows the properties of the desired object, in this case the TopSecret folder.

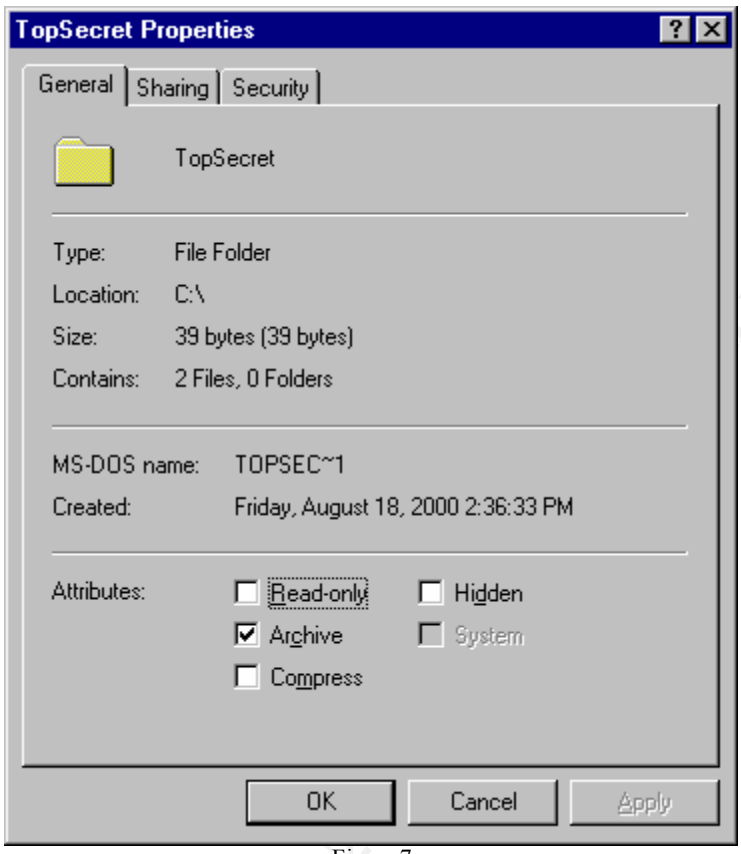


Figure 7

Click on and open the Security tab to enable auditing on the folder. Figure 8 below, demonstrates the options available on the Security tab.

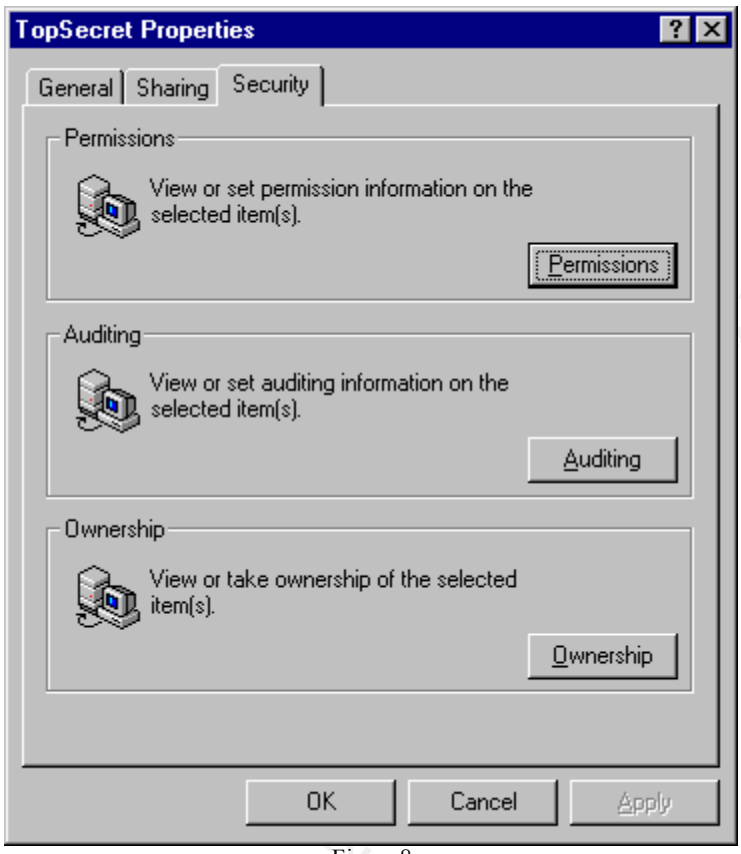


Figure 8

Click on the auditing button to open the screen displayed in Figure 9 below. As you can see, as is the case for the system, there is no auditing enabled by default for folders created on Windows NT.

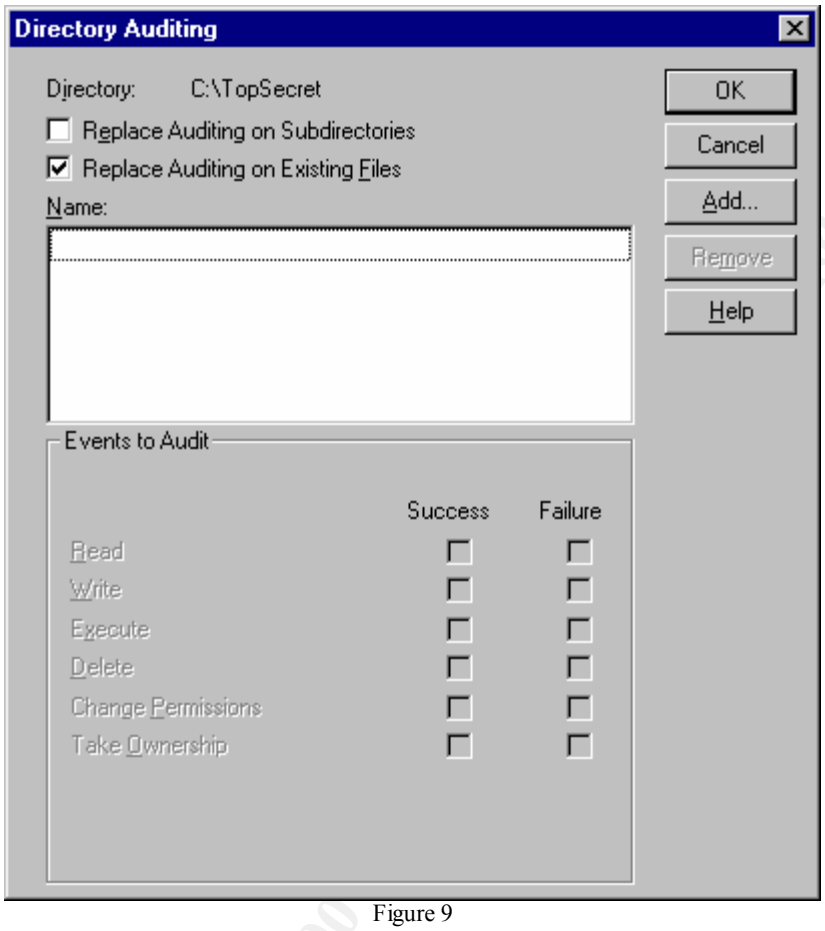


Figure 9

Suppose the need is to audit the actions of certain users or groups who have permission to access this folder. In order to do so, first click on the Add button. The result should be a screen similar to the one in Figure 10 below.

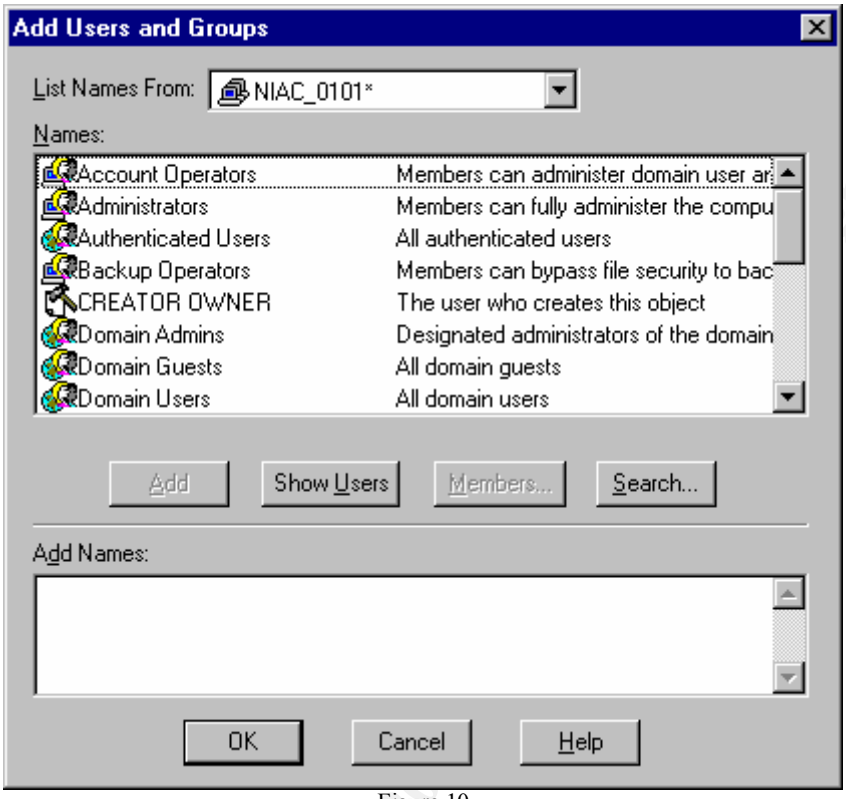


Figure 10

By default only group accounts are displayed initially in the top window of the screen. If the desire is to audit a particular user's access, click on the Show Users button and all user accounts will be displayed. In order to select a group or user account, highlight and double click on the account or highlight the account and click on the Add button. Select all user or group accounts to be audited. Each will be displayed in the bottom window as selected. In the example, Figure 11 below, three groups have been selected for auditing.

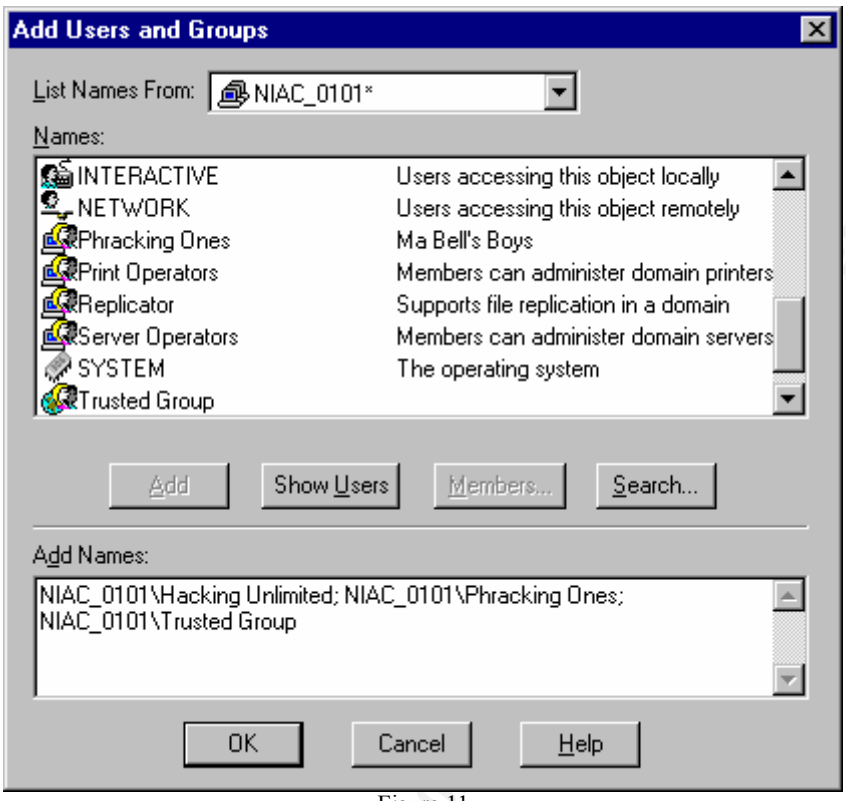


Figure 11

Once all desired selections are completed, click on the OK button at the bottom of the screen. As a result, a window similar to the one in Figure 12 below will be displayed.

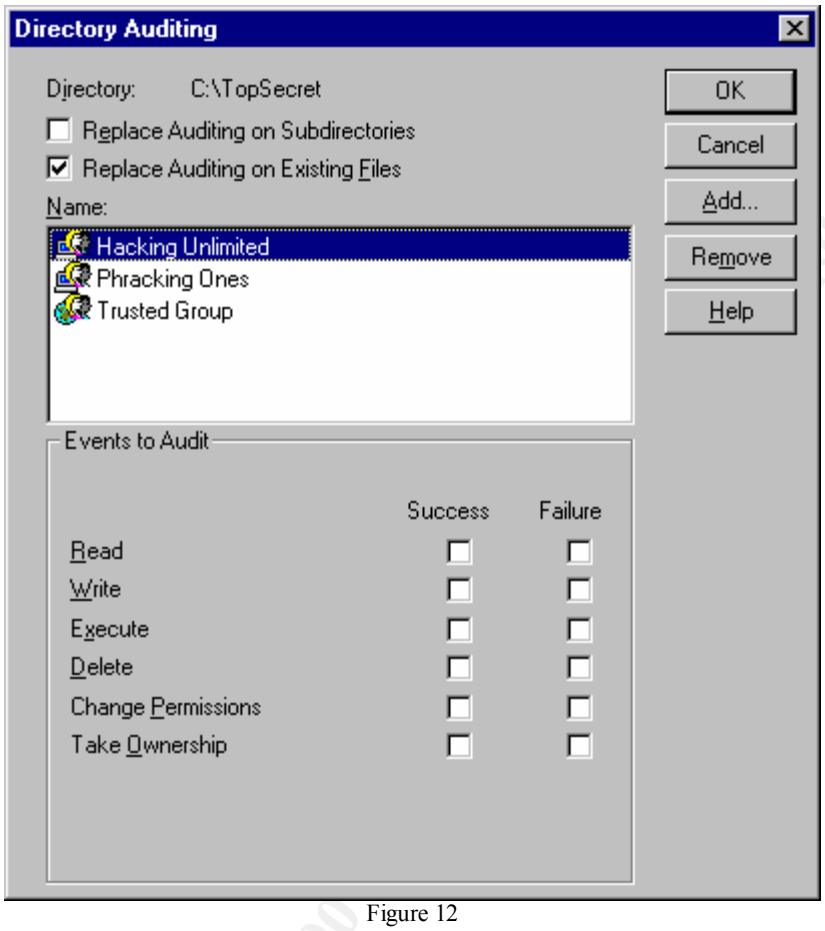


Figure 12

This is where an Administrator can make what could be a costly mistake in terms of auditing access to an object. In the example, Figure 12 above, three groups have been identified for auditing of access to the TopSecret Folder. Next, the Administrator would identify the type(s) of access he or she wishes to audit for the groups. This is where misconceptions or mistakes can occur. The novice, inexperienced, or rushed Administrator might at this point identify events to be audited and believe that they will apply to all of the groups in the window. The reality is that events selected at this point, as portrayed in Figure 12, will only apply to the highlighted group, Hacking Unlimited. Figure 13 below, demonstrates selection of events to audit for Hacking Unlimited.

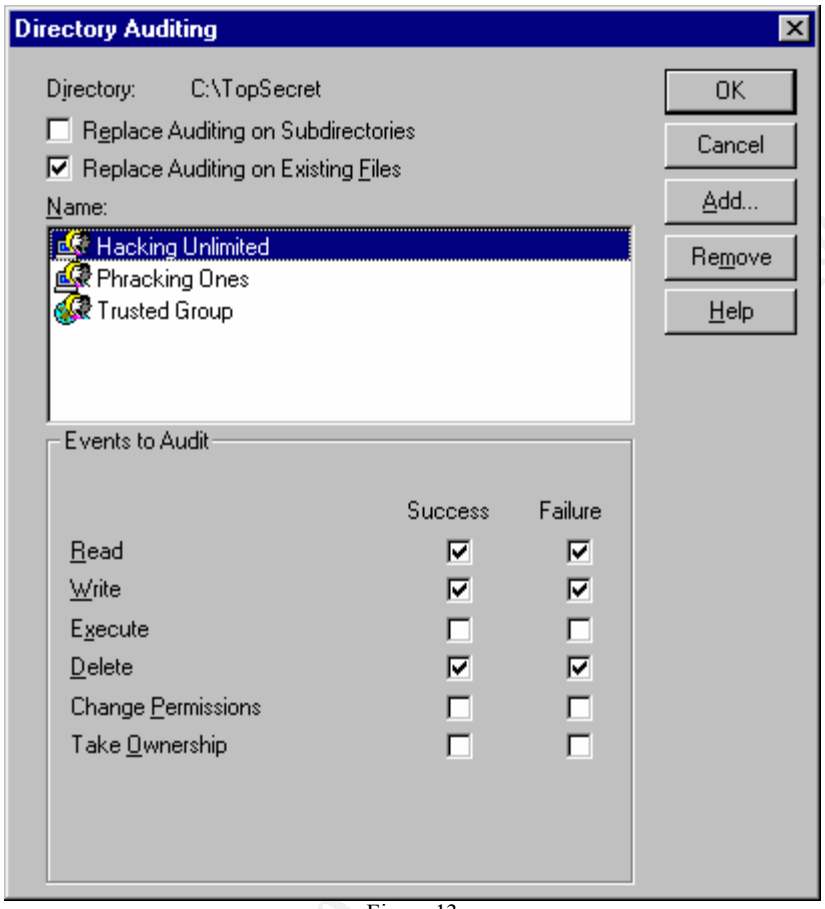


Figure 13

Again, the window portrayed in Figure 13 above can be deceiving to the inexperienced or hurried. It may appear that the auditing policy applies to all groups. At this point, the Administrator might click the OK button and assume that items identified will be audited for all groups in the window. If he or she did so, and were to reopen the audit window for the folder, Figure 14 below, depicts what the Administrator would see.

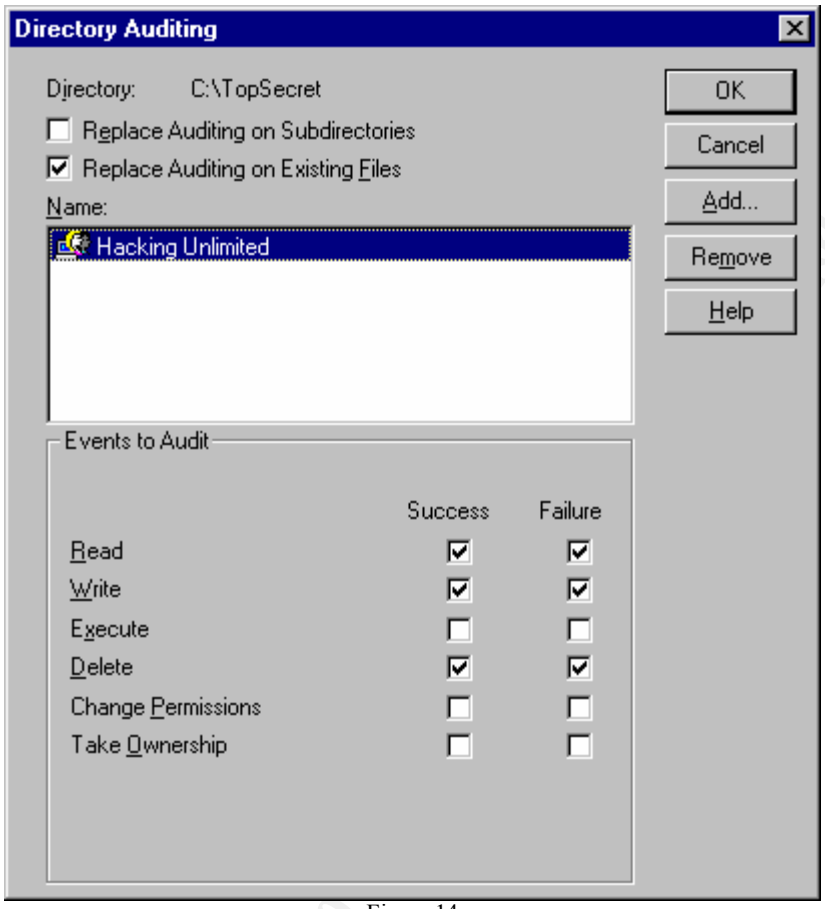


Figure 14

As you can see the other two groups are no longer even displayed in the window. The reason is that no events were selected for auditing for those groups. As a result, no record would ever be found in the Security Log indicating any access by Phracking Ones or Trusted Group (the other 2 groups thought to be audited) to the TopSecret Folder.

In order to set a policy for each group, it is necessary to highlight each group individually and then select events to audit. This also makes it possible to identify different items to audit for each group. Again, as Mr. Golias and Mr. Carboni demonstrated in their practical assignments, it may be a very good idea to ensure that your audit policy, whether at the system or object level, is indeed the policy that you intend. Had the policy been enabled as identified in Figure 13 and left unchecked, no access to TopSecret by either Phracking Ones or Trusted Group would have generated any events in the Security Log of Event Viewer.

Auditing a File Object

Assume now that the policy above (Figure 14) with the events identified had been appropriately applied to all three groups for the TopSecret Folder. The TopSecret Folder contains two files. I want to set an audit policy for one of the files. In order to set auditing at the file level open the properties of the file and select the Security tab. Click on the audit button.

Figure 15 below depicts the audit dialog box for the file.

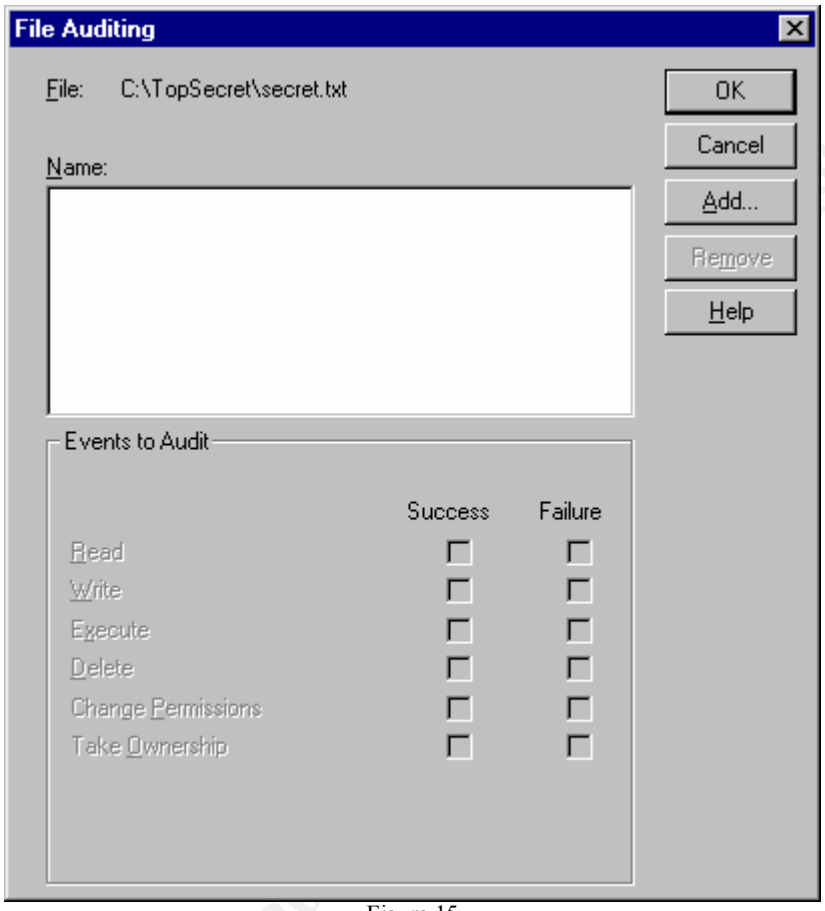


Figure 15

As with the folder, in order to add users or groups to audit, click on Add and make the appropriate selections.

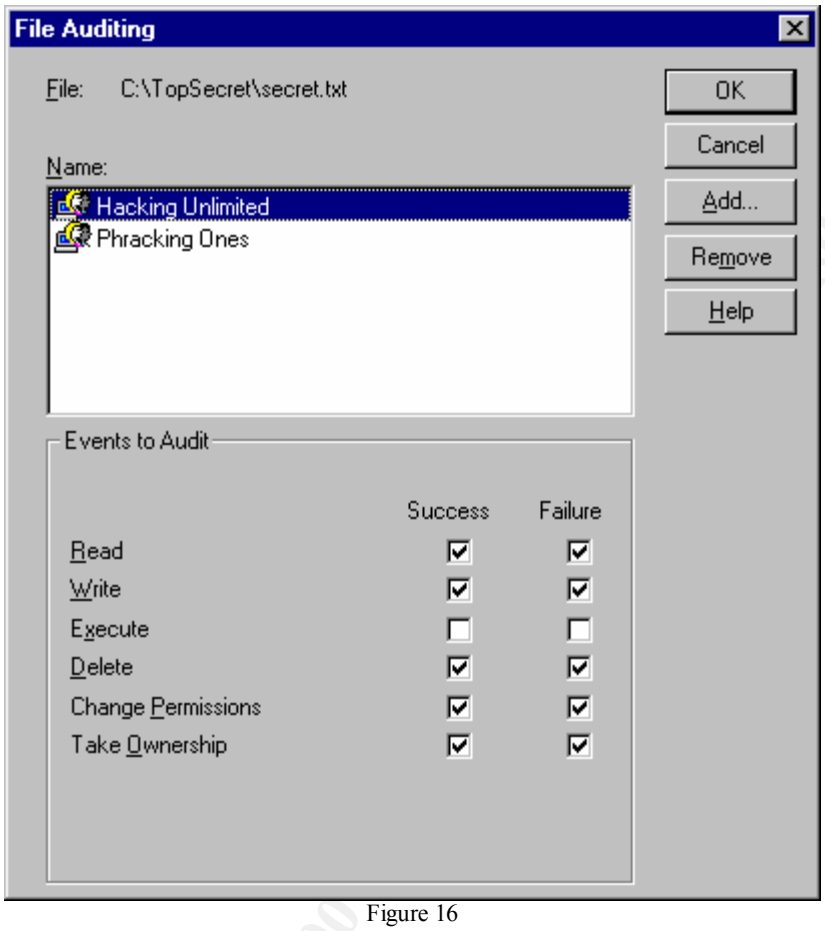


Figure 16

Assume I set auditing properly for the secret.txt file for both groups in the window in Figure 16 above for all events identified. A short time later the permissions to the file are changed. Assume further that only members of the Hacking Unlimited and Phracking Ones groups had permissions to access the file. I look in my Security Log and there is no event related to the change in permissions on the file. Why? I, as Administrators often do, made an oversight when setting up my auditing and did not verify the settings.

Let's take another look at the audit policy starting with the TopSecret folder. Auditing for TopSecret is shown in Figure 17 below.

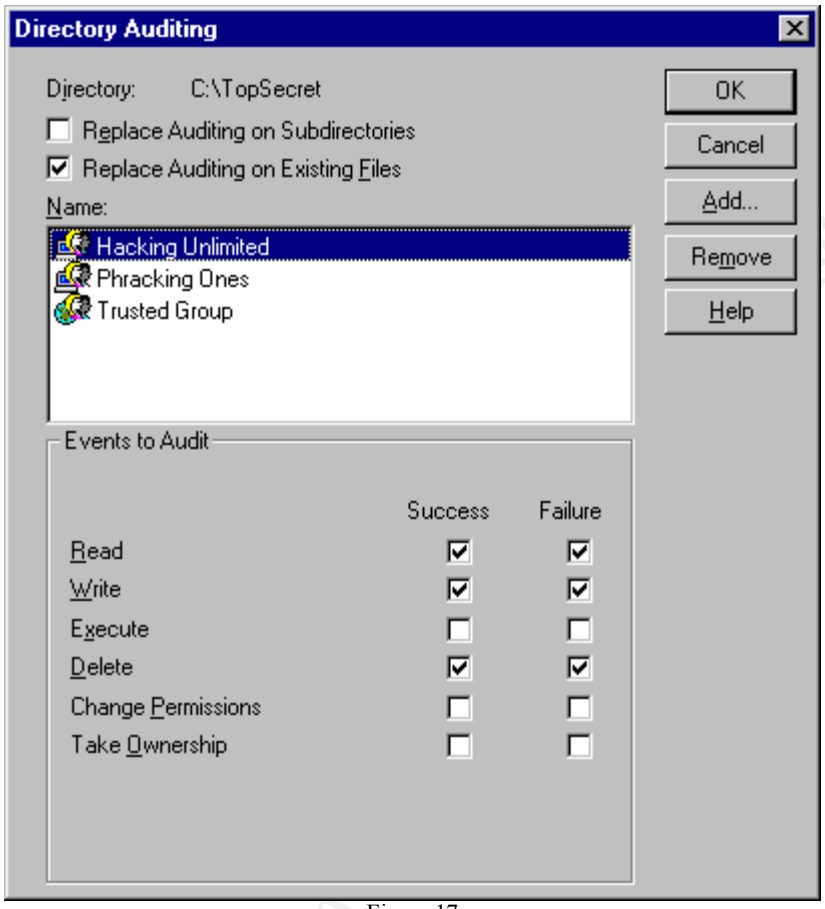


Figure 17

Again, assume that the events checked apply properly to each of the groups listed. The problem and reason that the change in permissions for the file did not generate an audit event in the Security Log is that the box Replace Auditing on Existing Files is checked at the folder level. I thought the audit policy for the file would be that as depicted in Figure 16. In actuality, after the auditing on files was replaced by the folder auditing policy, auditing for the file was that depicted in Figure 18 below.

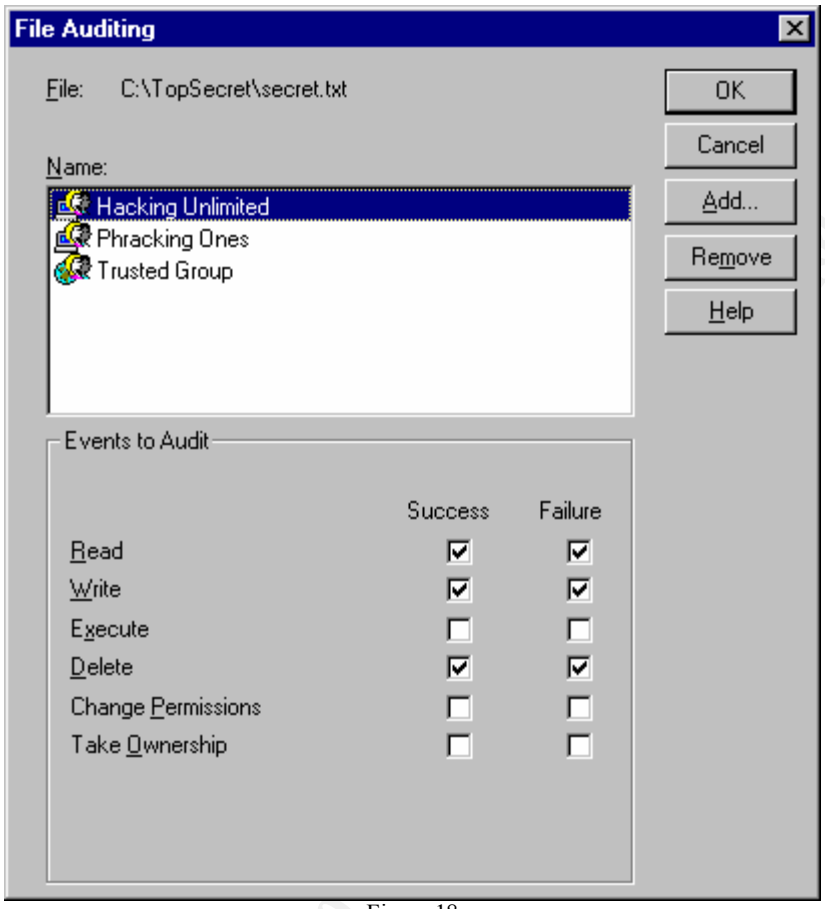


Figure 18

As you can see in the figure above there is no auditing for the Change Permission event.

Had I double checked, and ensured the policy was as I intended, I would have had an incident generated in the Security Log when the permissions to the secret.txt file were changed. If I intended a different policy for files than I had set at the folder level, I should have removed the check from the Replace Auditing on Existing Files box in the folder audit dialog box. Instead I am left with no evidence in the Security Log to indicate who changed permissions on the file.

Auditing User Accounts

Many organizations want to know exactly what user accounts are used to logon to their systems at any given time. Accordingly, the Logon and Logoff item, for both Success and Failure, will be selected for audit in the User Manager for Domains audit policy.

Missing Failed Logon Attempts in Security Log of PDC

A large number of failed logon attempts should cause concern. They could be an indication that someone is trying to hack into your system. Administrators should be vigilant at tracking numerous failed logons and attempt to determine the cause. Thus many Administrators will examine their PDC Security Log daily looking for failed logon attempts. Unfortunately, I have come across Administrators who are not aware that, "due

to an inexplicable decision by Microsoft, a failed logon to a domain from an NT workstation will only log a security event to the workstation (if auditing for logon events is enabled) attempting to connect, rather than to a domain controller."[9] Upon learning of this fact myself, I was rather skeptical. I conducted the appropriate testing and sure enough this is true. The following screenshots and explanations will demonstrate the fact.

\\STUDENT16 is an NT Workstation that has an account on \\INSTRUCTOR, a PDC. I first enabled the user account, also named student16, and attempted to logon from Workstation \\STUDENT16 to ensure success. Figure 19 below, demonstrates that at 2:38:36 PM on 2/3/01 user account student16 was used to successfully log on to the PDC from Workstation \\STUDENT16.

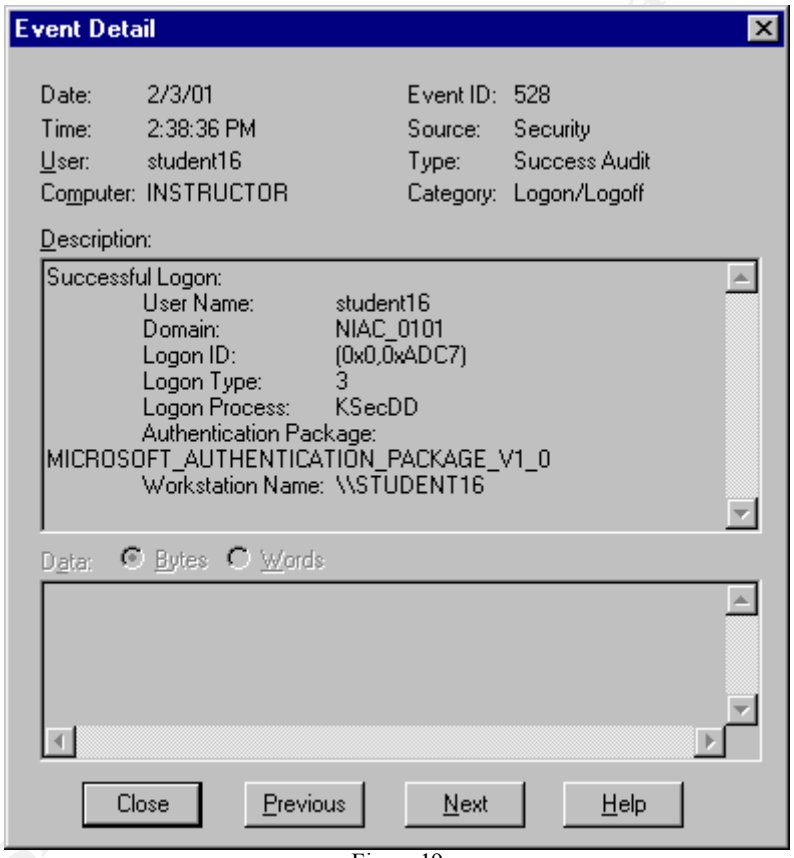


Figure 19

After ensuring the ability to logon successfully, I logged off. I then used the same account and workstation to make several failed attempts, using the wrong password, to once again logon to the PDC. After exceeding the account lockout threshold on the PDC (4 bad attempts) the student16 user account was locked out. The following screenshots, Figures 20 and 21, are from the PDC's Security Log. In reference to the failed logon

[9] Scott, Cory L. "Dealing with Windows NT Event Logs Part 2" http://www.securityfocus.com/ (page 2)

attempts, Figure 20 indicates only a Success Audit (highlighted), that being the User Account Locked Out. Figure 21 is the screenshot of the details of the highlighted event.

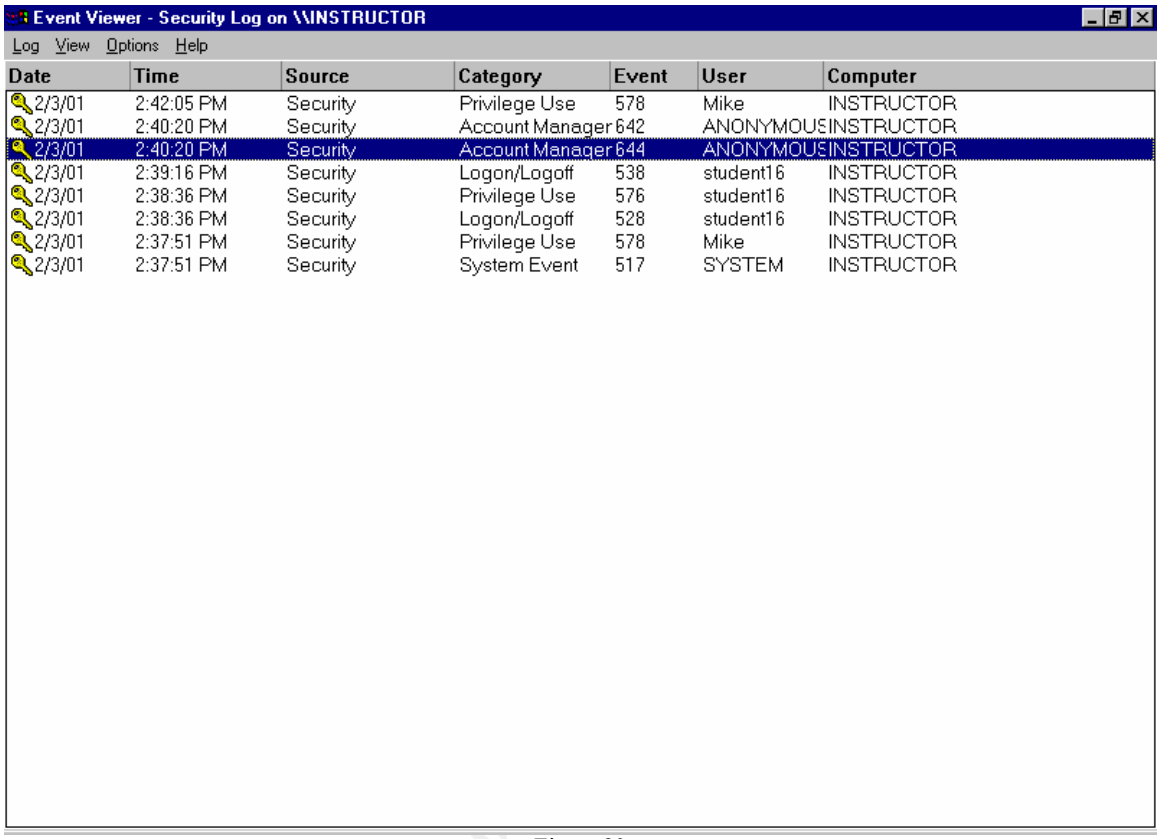


Figure 20

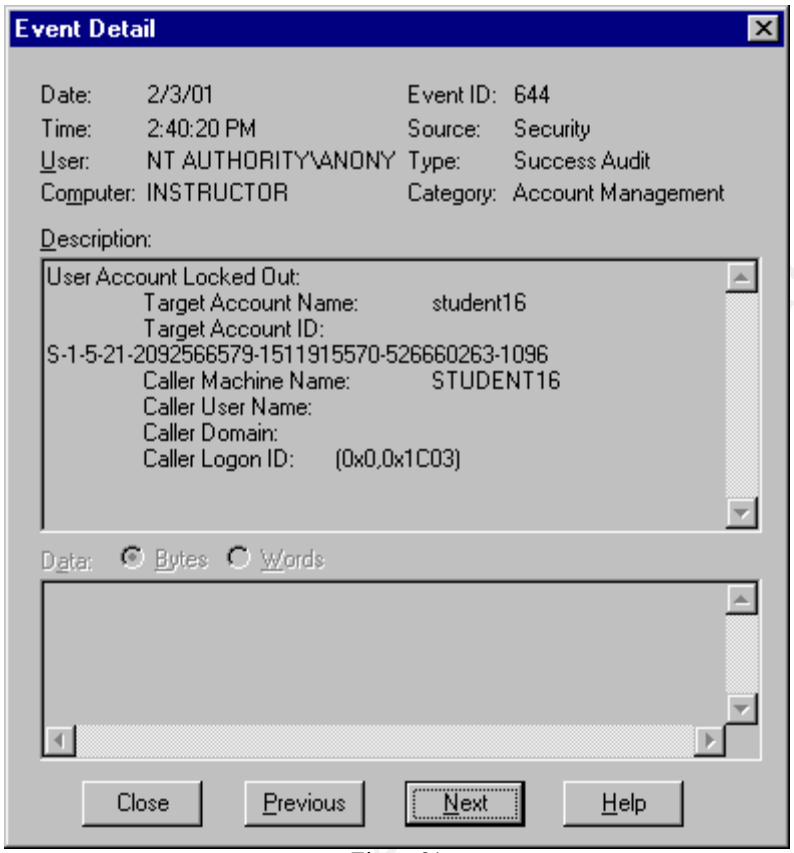


Figure 21

First, it should be noted that if not for Account Lockout having been enabled in the Account Policy on the PDC, there would be no indication of the failed logon attempts in the PDC Security Log. If Account Lockout is not enabled, someone with a list of user accounts could use the accounts to make an infinite number of attempts to logon to a PDC from an NT Workstation by guessing passwords and never generate any incident in the PDC Security Log that raises an alarm.

Even with Account Lockout enabled malicious attempts to logon to the PDC may go unnoticed. I have met Administrators who indicate that they only have time for a cursory scan of logs and it is common to look for failed attempts only, or the lock icon, when reviewing a PDC Security Log. (A better practice may be to scan for events by number). If this is the case, they may never even notice the successful audit of the Account Lockout. Thus they would never know about the failed attempts to logon unless the owner of a locked out account inquired as to why the account was locked out. Worse still, by default, when Account Lockout is enabled it is only after 5 bad attempts and then only for 30 minutes, not forever. Unless this default is changed the account lockout may conceivably go unnoticed all together if the legitimate user does not attempt to logon within 30 minutes of lockout.

Figure 22 below, is the Security Log from NT Workstation \\STUDENT16. The highlighted incident is the fourth bad attempt to logon to the PDC by user account

student16 from the workstation. Notice that the time corresponds exactly with the account lockout time generated in the Security Log of the PDC (Figure 21).

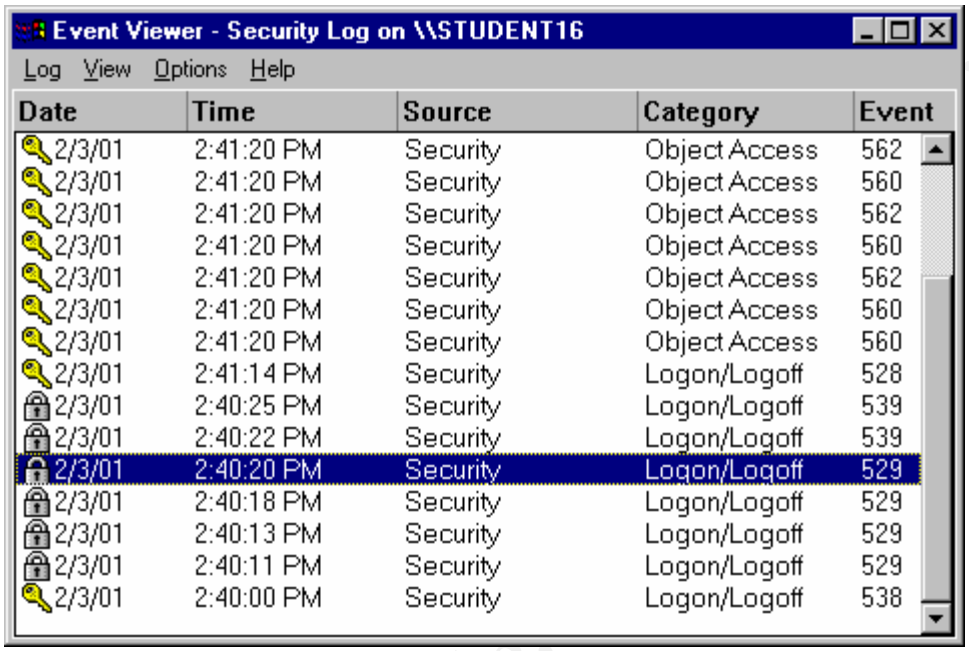


Figure 22

Figure 23 below, depicts the details of the incident highlighted in Figure 22 above.

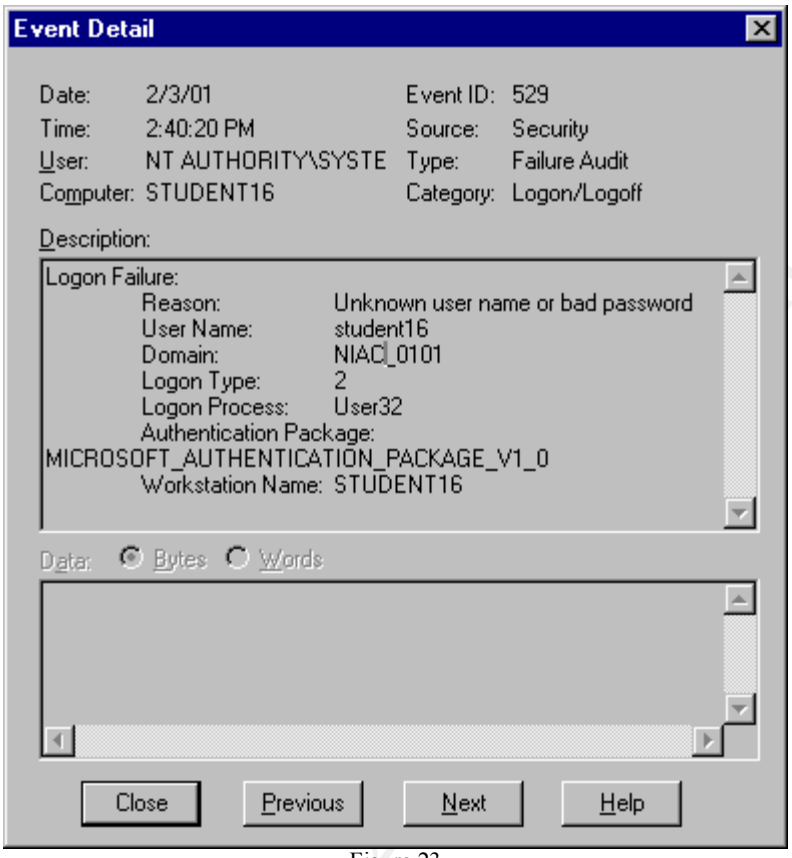


Figure 23

Obviously, if Logon and Logoff Failures were not enabled on the NT Workstation there would not even have been an event generated in the workstation Security Log and thus no record of the failed attempts to logon to the PDC with the student16 account from NT Workstation \\STUDENT16.

The fact that failed logon attempts from an NT Workstation to a PDC only generate an event in the Security Log of the workstation, if auditing is enabled properly on the workstation, makes it imperative that Administrators have a system for compiling and examining logs from multiple machines.

Evidence of Failed Attempt to Logon as Administrator

As a side note, assume the Failure option for the Logon and Logoff item is not being audited on the system. If this is the audit policy on your system and a user were to gain physical access and attempted to logon by guessing the Administrator's password, you would have no indication in the Security Log. Remember the Administrator account cannot be locked out. A potential intruder could make as many guesses as time permits and you may never know because there will be no events in the logs to provide any indication.

However, if account lockout has been enabled in the account policy in User Manager for Domains, NT will provide evidence of failed attempts to access the Administrator's account. The attempts would have had to exceed the threshold of the account lockout

policy. For instance assume account lockout was configured as indicated in Figure 24 below. Making 5 failed attempts to logon as the Administrator in less than 30 minutes will cause a check to be placed in the Account Locked Out box of the Administrator's account properties dialog box.

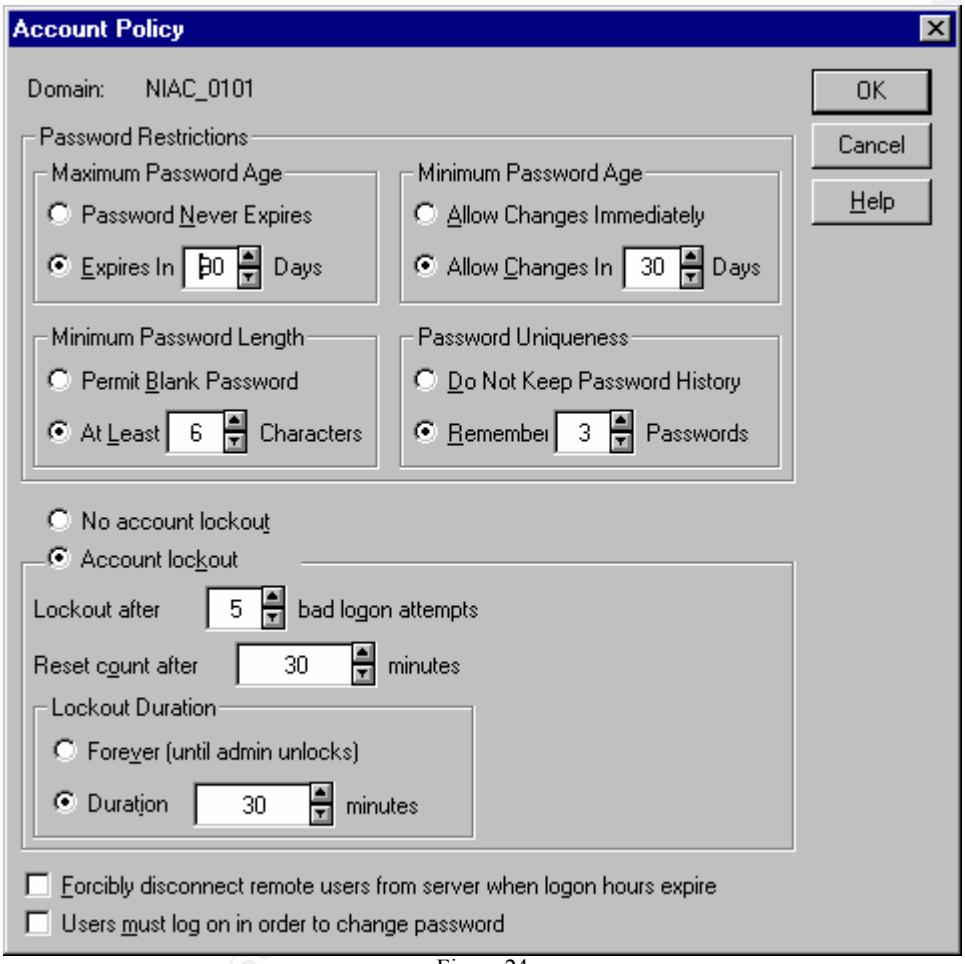


Figure 24

Figure 25 depicts the Administrator's User Properties window prior to 5 failed attempts to logon. You may notice that the Administrator account name has been changed to Mike. Although not the name I would use on an actual system it is a good idea to change the name of the Administrator account to something less conspicuous. As Jeff Payne points out in Section 3c of his practical, "The account should be changed to a different name which will add another hurdle for intruders to overcome."[10] I would further Mr. Payne's suggestion for changing the account by removing the information in the Description field as I have done in this example. I assure you this is the Administrator account. Please try what I describe on your own system with your Administrator account.

[10] Payne, Jeff "Practical Assignment For SANS Security Monterey 2000" http://www.sans.org/giactc/gcnt.htm

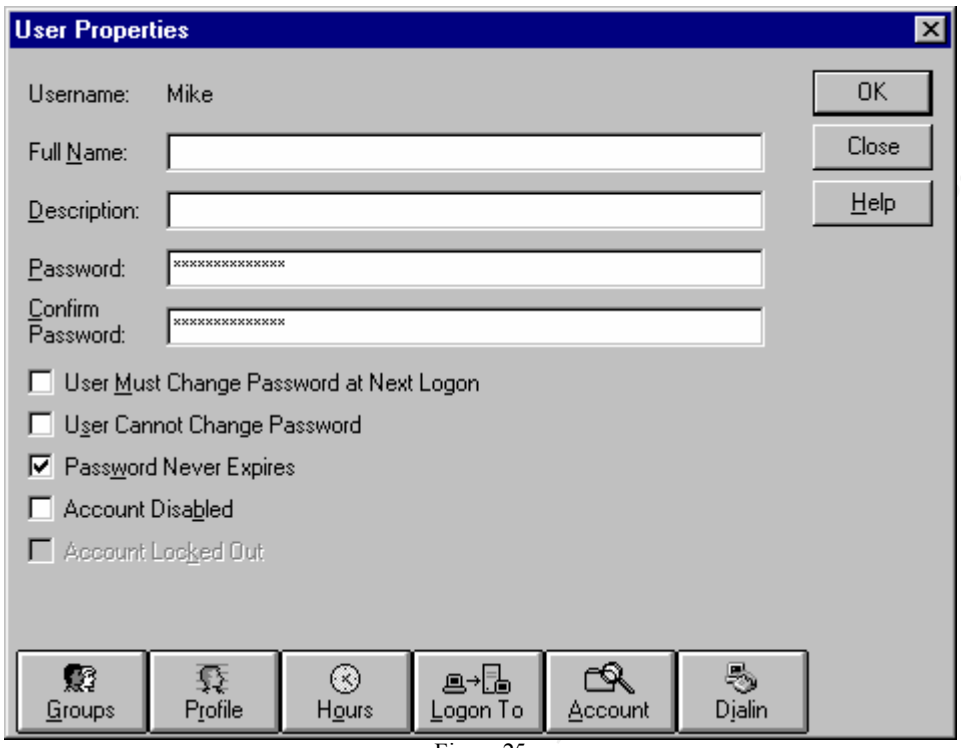


Figure 25

Figure 26 depicts the Administrator's properties window after the 5 failed attempts to logon in less than 30 minutes. Notice the checkmark in the Account Locked Out box.

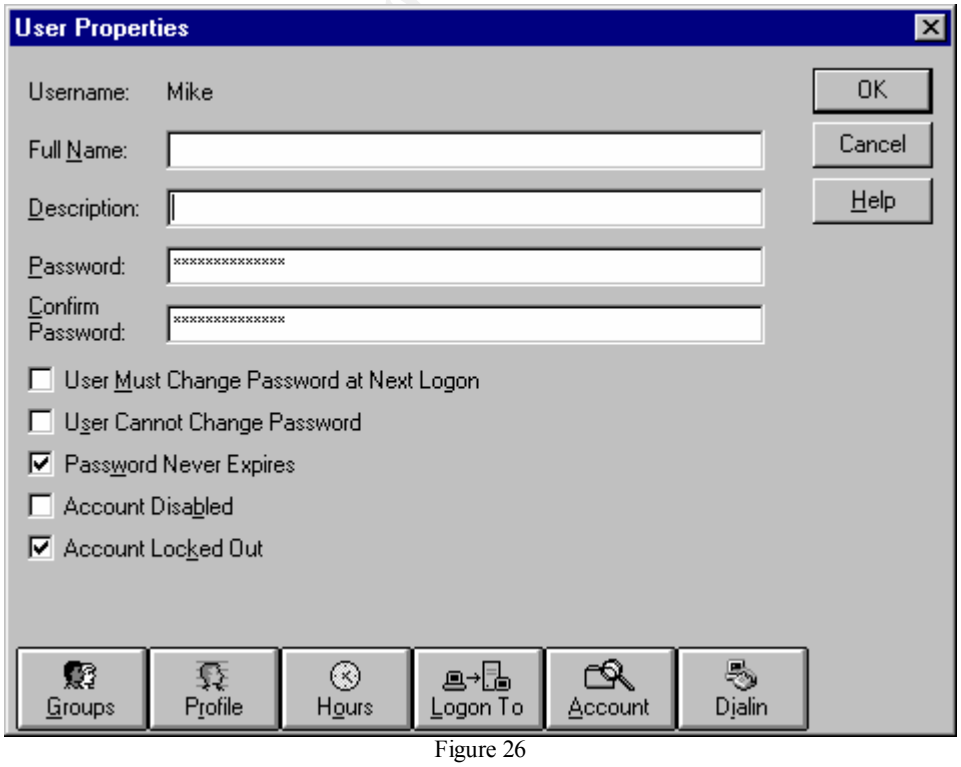


Figure 26

The Administrator's account was not actually locked out. However, the check in the Account Locked Out box does indicate that someone used the account to attempt to logon and failed at least enough times to exceed the Account Lockout threshold. It does not mean that the individual was not eventually successful. It should warrant further investigation.

In his practical assignment Justin Saxinger states, "Extra attention should be paid to events such as numerous failed logon attempts, a failed logon attempt with the Administrator account or changes to the Administrators group."[11] I would further suggest adding the check I refer to above to monitoring of the Administrator account.

Event Viewer logs will not always be complete. Administrators should be aware of other ways to gain information if available and required.

Determining Last Logon for a User Account

If there is no Logon and Logoff auditing enabled on the system and there is a need to know the last time a user logged on, there are other ways to ascertain that information.

net user

Open a Command Prompt window and enter "net user" followed by an account name. Figure 27 below, displays the command and resulting information displayed.

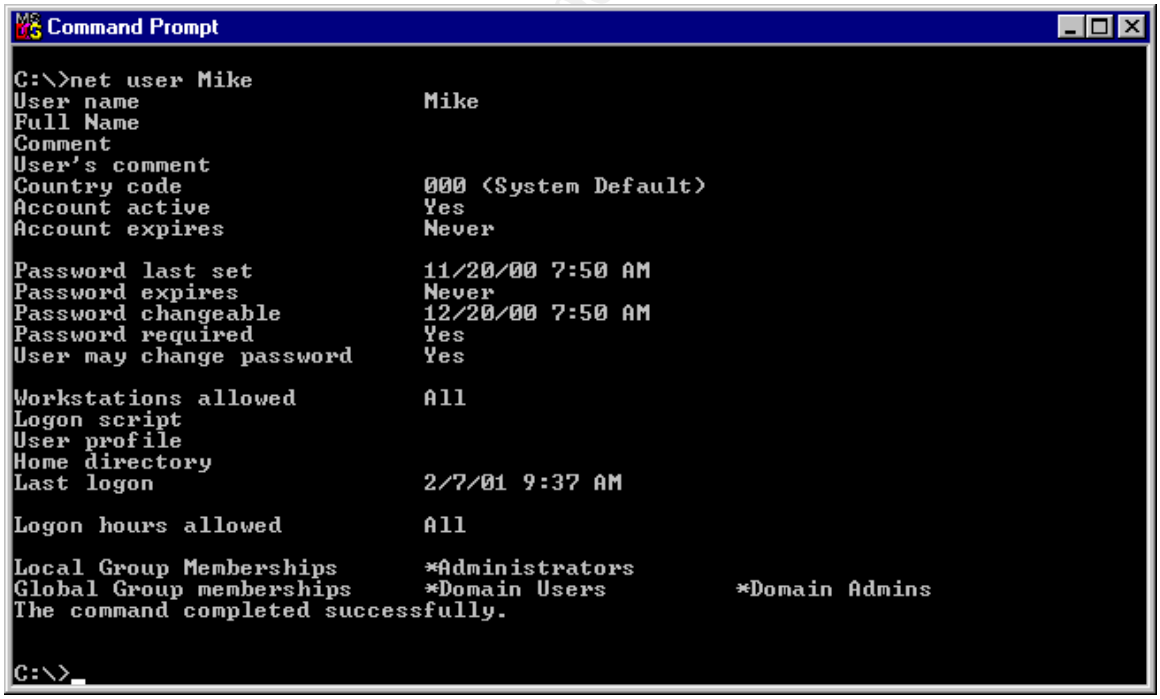


Figure 27

[11] Saxinger, Justin "Essential Steps for Securing a Windows NT 4 Server" http://www.sans.org/y2k/practical/Justin_Saxinger_GCNT.doc

DumpSec

Additionally, this information could be obtained using the DumpSec tool referred to early in this document. After executing DumpSec, click on Report on the toolbar and Dump Users as table as in Figure 28 below.

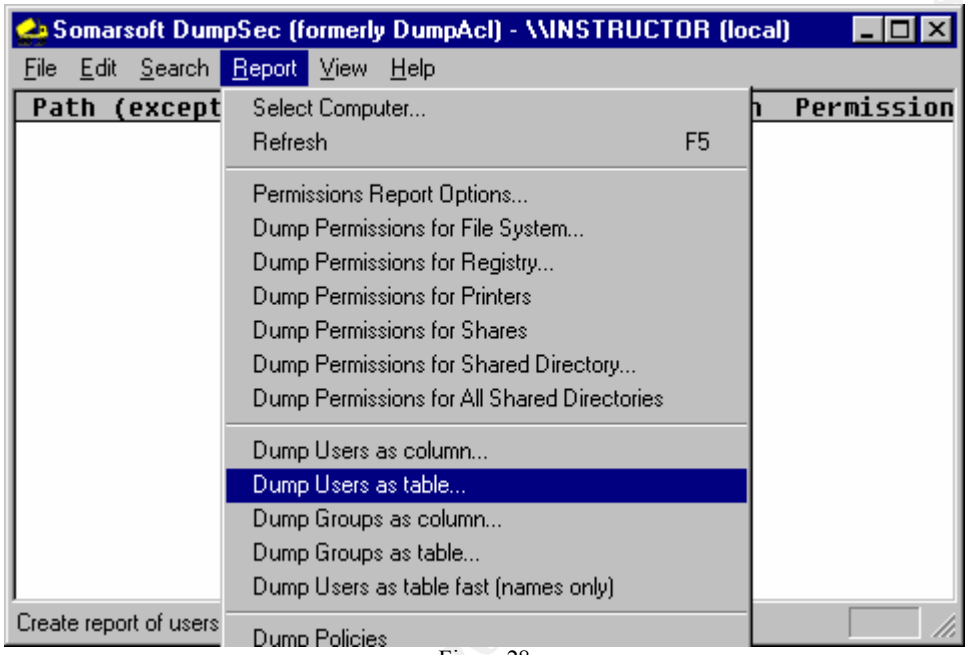


Figure 28

Make the appropriate selection from the left panel and Add them to the Selected fields window on the right as in Figure 29 below.

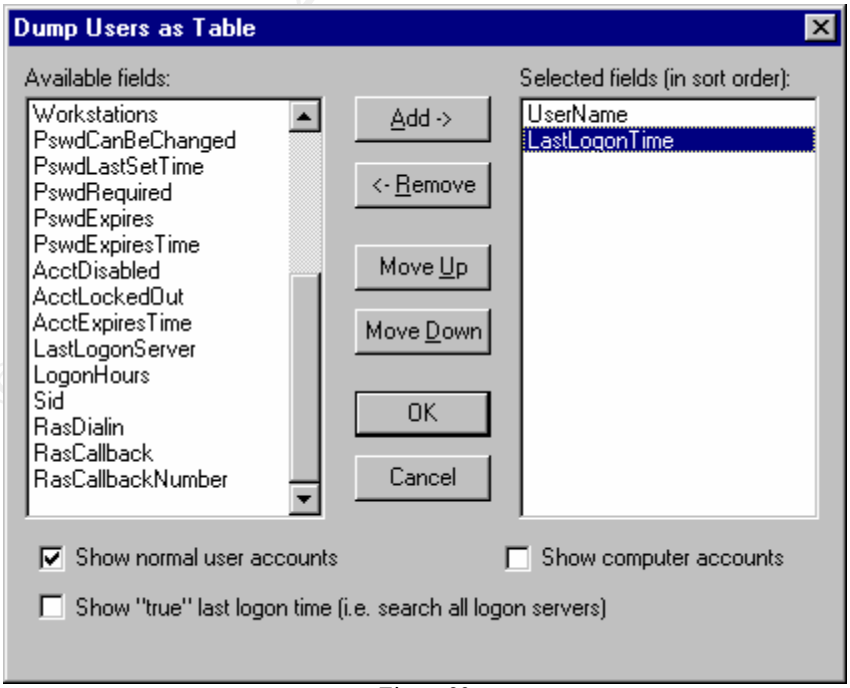


Figure 29

Figure 30 below, depicts the information desired by selections made in Figure 29 above.

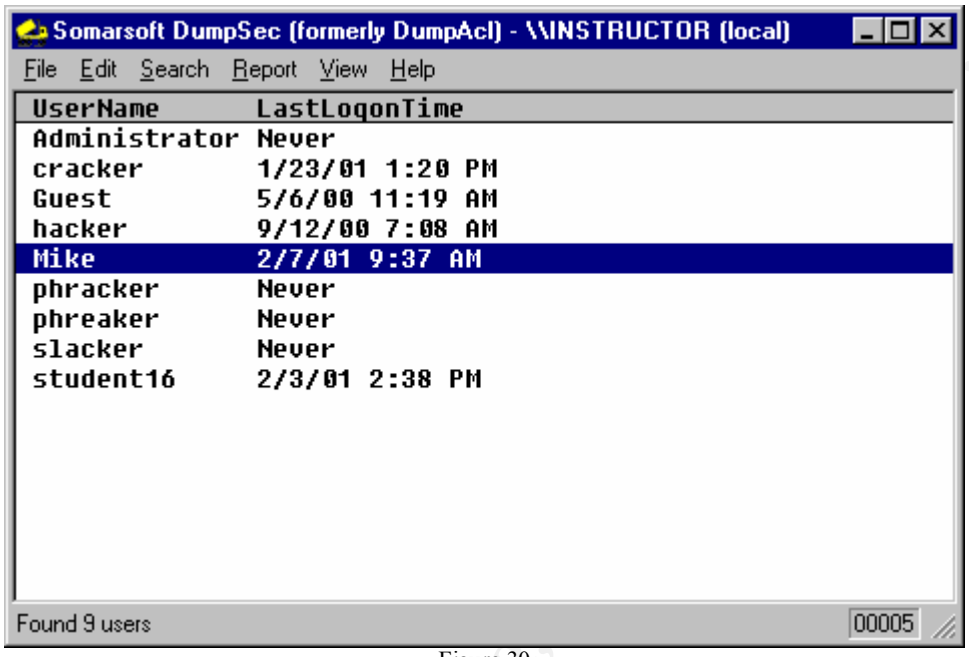


Figure 30

Lack of complete logs – Missing Entries

There may be a number of reasons for incomplete, or seemingly incomplete, Windows NT log files. It could be that a hacker has managed to stop auditing, cleared the logs, or it could be that logs are missing for reasons that are not related to maliciousness.

Is Auditing Enabled?

If logging appears to have ceased it may be prudent to first check the audit policy in User Manager for Domains to ensure auditing is still enabled at the system level.

Is EventLog Service Started?

Check the EventLog service to ensure that it has not been stopped. This can be done through the Services icon in Control Panel. In Figure 31 below, you can see that the service has started. Under Windows NT 4.0 the service cannot be stopped or paused while the system is up and running. However, it can be configured to be disabled or stopped on startup. This is another reason to be concerned about and perhaps audit Restart, Shutdown, and System in User Manager for Domains Audit policy.

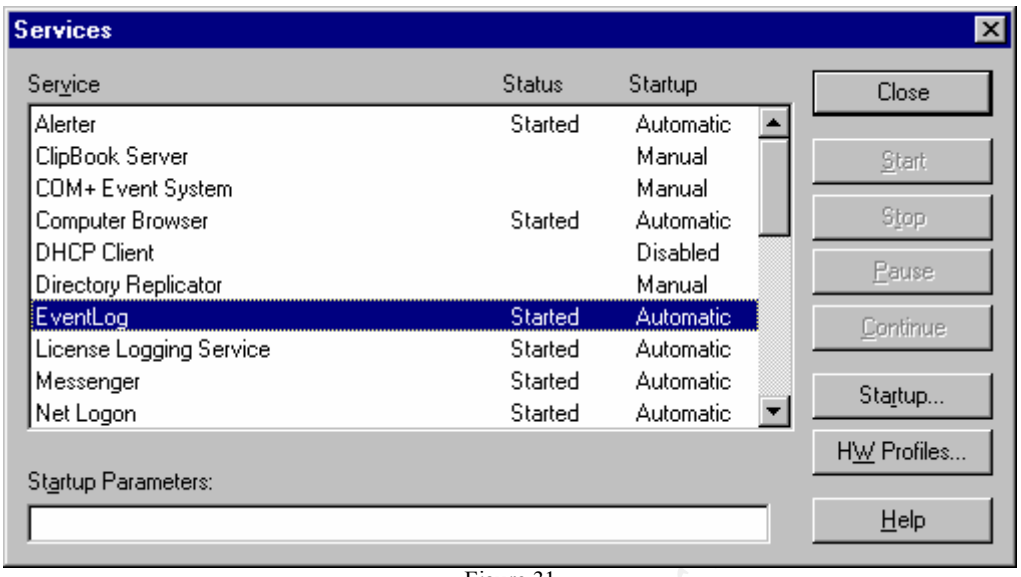


Figure 31

How is Event Log Wrapping Configured?

You must also consider how Event Log Wrapping is configured in the Event Viewer Application. More often than not, this may provide the answer to why logs appear to be missing. Open the Event Viewer Application and click on Log on the toolbar and Log Settings in the drop-down menu as demonstrated in Figure 32 below.

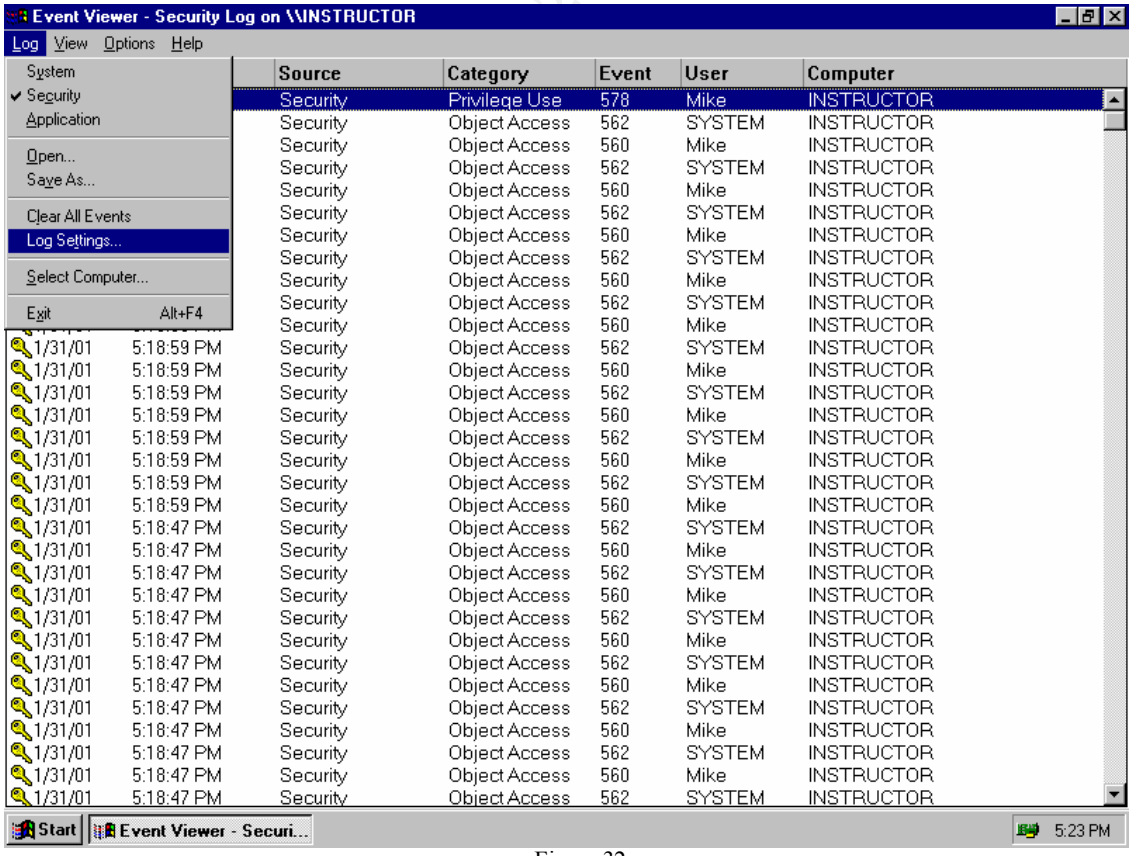


Figure 32

Figure 33 below depicts the Log Settings window.

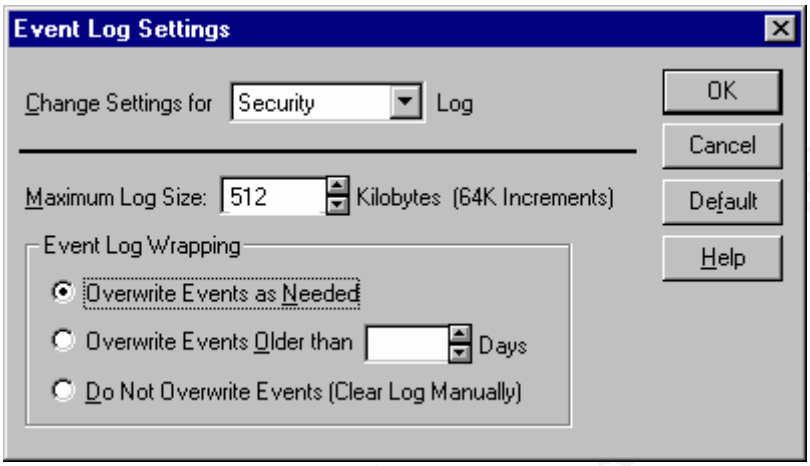


Figure 33

There are three options to choose from for Event Log Wrapping.

Overwrite Events as Needed
This is the default setting. The newest events will simply overwrite the oldest events if the log is full.

Overwrite Events Older than N Days
N is a setting between 1-365 days. If there are no events in a filled log file older than the number specified, NT will discard new logs and they will be lost.

Do Not Overwrite Events (Clear Log Manually)
No new events will be added to the log and will be lost when the log is full.

Obviously, your particular situation will dictate which option for Event Log Wrapping will be best. However, there are some factors that all Administrators should take into consideration when deciding on which option to use. The wrong choice may be the reason for incomplete logs.

Before deciding Log Setting configuration, a baseline should be established to determine how quickly incidents are generated on the system and thus, how quickly logs fill. The baseline will allow you to determine how much space should be reserved for logging. Without this research it is possible to devote too little space to logging which could result in lost data depending on which Event Log Wrapping option is chosen and your backup policy, if one exists.

Consider the first option, the default setting, Overwrite Events as Needed. If the audit policy results in the logs filling the default 512K of space in an average of 2 days, there is a good chance that there will never be more than 2 days worth of data in the default size log. If logs were not saved and archived (another issue) at a minimum of every 48 hours, crucial data could easily be lost. With this setting it is also easy for a malicious user to

generate logs in order to overwrite events and cover tracks even if additional space has been allocated for logs.

If the second option is used with the default space allocated for logging, there is a good chance of losing data on heavily used systems. With this option, it is again, important to establish a baseline to determine how quickly the logs fill. When this option is chosen, the default is to overwrite events older than 7 days. If the logs fill the allocated space in 2 days, no subsequent events will be logged until the system finds an event older than 7 days to overwrite. In this case, 5 days of data could potentially be lost.

If the last option is chosen and the log reaches maximum allocated space, new events are not added to the log and are lost. The log must be cleared manually before logging can resume. A message indicating which log is full will appear as a warning to the Administrator. The Administrator's intervention is required before logging will continue. In the meantime new incidents will be lost. Of course the system can be configured to crash when the security log is full. For more information on this option please see the practical assignments by Ruth Parish[12] and Howard F. Gabert.[13]

The default log size of 512K can be increased. Each of the log files can theoretically be allocated 4Gb of space. However, I add the following caveat by James D, Murray. "You must also avoid specifying a very large maximum log file size. The larger a log file is, the slower it is to search, and the more memory and resources are required to use and maintain it. Although 4Gb is the maximum log size allowed by Event Viewer, the log files will probably not grow to more than 300Mb in size due to the limitations in a system's configuration and in Windows NT. To maintain a responsive system, you should specify a maximum log file size that is considerably less."[14]

Knowing your system, establishing a baseline and monitoring are ways to ensure you allocate the proper amount of space for logs and use the appropriate Event Log Wrapping option so you do not lose events.

Viewing Logs with Event Viewer

Thousands of log entries can be generated in a very short period of time depending on how many events and objects are under audit and how many accounts are accessing resources. Few, if any, Administrators have the time to scan thousands of entries on a daily basis. Windows NT logs can be filtered when viewed with the Event Viewer Application. As mentioned early in this document it may be wise to filter for certain events if time for reviewing logs is limited. I will very briefly discuss and demonstrate viewing logs using the filtering option. To demonstrate filtering I created a few log

[12] Parish, Ruth Anne "An In-Dept Examination of Event Viewer and Auditing" http://www.s1ans.org/y2k/practical/Ruth_Anne_Parish_GCNT.doc (page 8)

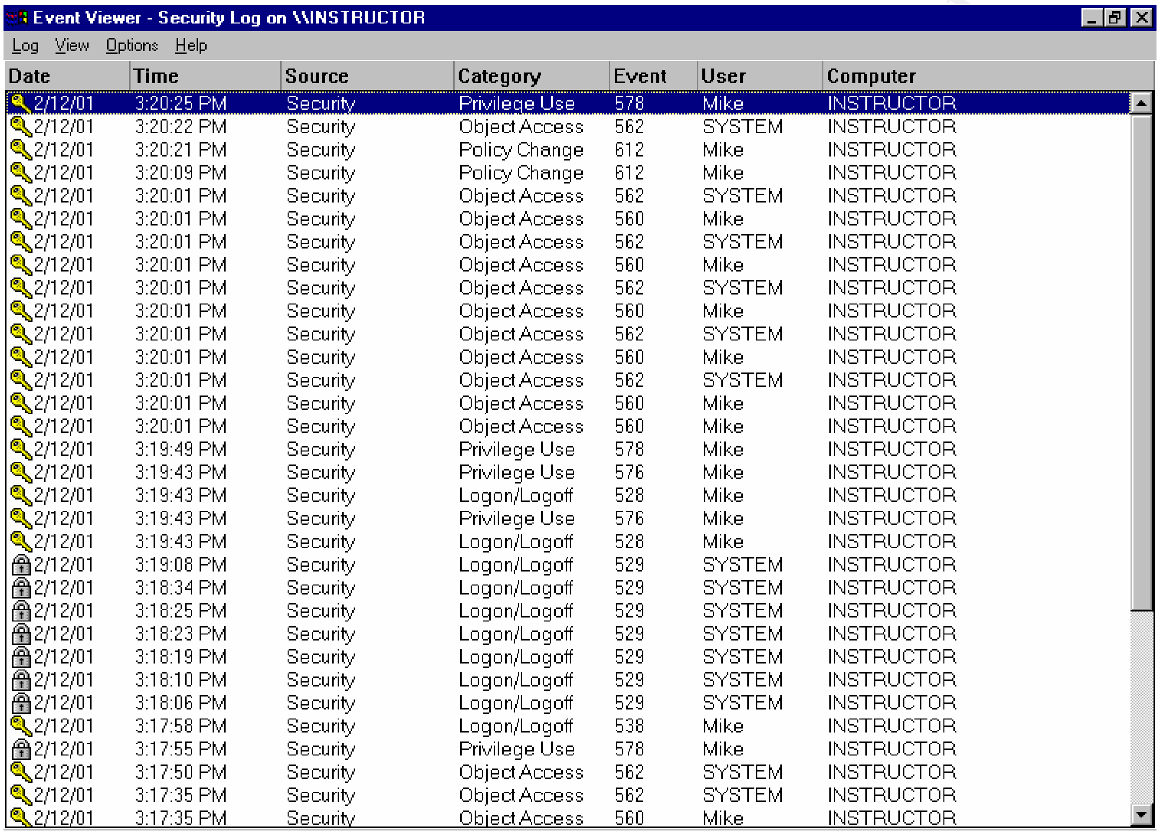
[13] Gabert, Howard F. "Using Event Logs to Audit Windows NT4" http://www.sans.org/y2k/practical/Howard_Gabert.doc (page5)

[14] Murray, James D. *Windows NT Event Logging* (O'Reilly & Associates, 1998) page 51.

entries in my Security Log. The entries were created in the span of about 4 minutes. This is just for demonstration purposes. Obviously, actual logs could span days or weeks and include thousands of entries or more.

Enable Filtering

In order to use filtering with Event Viewer, first open the desired log as in Figure 34 below, in this case the Security Log.



Date	Time	Source	Category	Event	User	Computer
2/12/01	3:20:25 PM	Security	Privilege Use	578	Mike	INSTRUCTOR
2/12/01	3:20:22 PM	Security	Object Access	562	SYSTEM	INSTRUCTOR
2/12/01	3:20:21 PM	Security	Policy Change	612	Mike	INSTRUCTOR
2/12/01	3:20:09 PM	Security	Policy Change	612	Mike	INSTRUCTOR
2/12/01	3:20:01 PM	Security	Object Access	562	SYSTEM	INSTRUCTOR
2/12/01	3:20:01 PM	Security	Object Access	560	Mike	INSTRUCTOR
2/12/01	3:20:01 PM	Security	Object Access	562	SYSTEM	INSTRUCTOR
2/12/01	3:20:01 PM	Security	Object Access	560	Mike	INSTRUCTOR
2/12/01	3:20:01 PM	Security	Object Access	562	SYSTEM	INSTRUCTOR
2/12/01	3:20:01 PM	Security	Object Access	560	Mike	INSTRUCTOR
2/12/01	3:20:01 PM	Security	Object Access	562	SYSTEM	INSTRUCTOR
2/12/01	3:20:01 PM	Security	Object Access	560	Mike	INSTRUCTOR
2/12/01	3:20:01 PM	Security	Object Access	562	SYSTEM	INSTRUCTOR
2/12/01	3:20:01 PM	Security	Object Access	560	Mike	INSTRUCTOR
2/12/01	3:20:01 PM	Security	Object Access	560	Mike	INSTRUCTOR
2/12/01	3:19:49 PM	Security	Privilege Use	578	Mike	INSTRUCTOR
2/12/01	3:19:43 PM	Security	Privilege Use	576	Mike	INSTRUCTOR
2/12/01	3:19:43 PM	Security	Logon/Logoff	528	Mike	INSTRUCTOR
2/12/01	3:19:43 PM	Security	Privilege Use	576	Mike	INSTRUCTOR
2/12/01	3:19:43 PM	Security	Logon/Logoff	528	Mike	INSTRUCTOR
2/12/01	3:19:08 PM	Security	Logon/Logoff	529	SYSTEM	INSTRUCTOR
2/12/01	3:18:34 PM	Security	Logon/Logoff	529	SYSTEM	INSTRUCTOR
2/12/01	3:18:25 PM	Security	Logon/Logoff	529	SYSTEM	INSTRUCTOR
2/12/01	3:18:23 PM	Security	Logon/Logoff	529	SYSTEM	INSTRUCTOR
2/12/01	3:18:19 PM	Security	Logon/Logoff	529	SYSTEM	INSTRUCTOR
2/12/01	3:18:10 PM	Security	Logon/Logoff	529	SYSTEM	INSTRUCTOR
2/12/01	3:18:06 PM	Security	Logon/Logoff	529	SYSTEM	INSTRUCTOR
2/12/01	3:17:58 PM	Security	Logon/Logoff	538	Mike	INSTRUCTOR
2/12/01	3:17:55 PM	Security	Privilege Use	578	Mike	INSTRUCTOR
2/12/01	3:17:50 PM	Security	Object Access	562	SYSTEM	INSTRUCTOR
2/12/01	3:17:35 PM	Security	Object Access	562	SYSTEM	INSTRUCTOR
2/12/01	3:17:35 PM	Security	Object Access	560	Mike	INSTRUCTOR

Figure 34

Next click on View in the toolbar and Filter Events in the drop-down menu as in Figure 35 below.

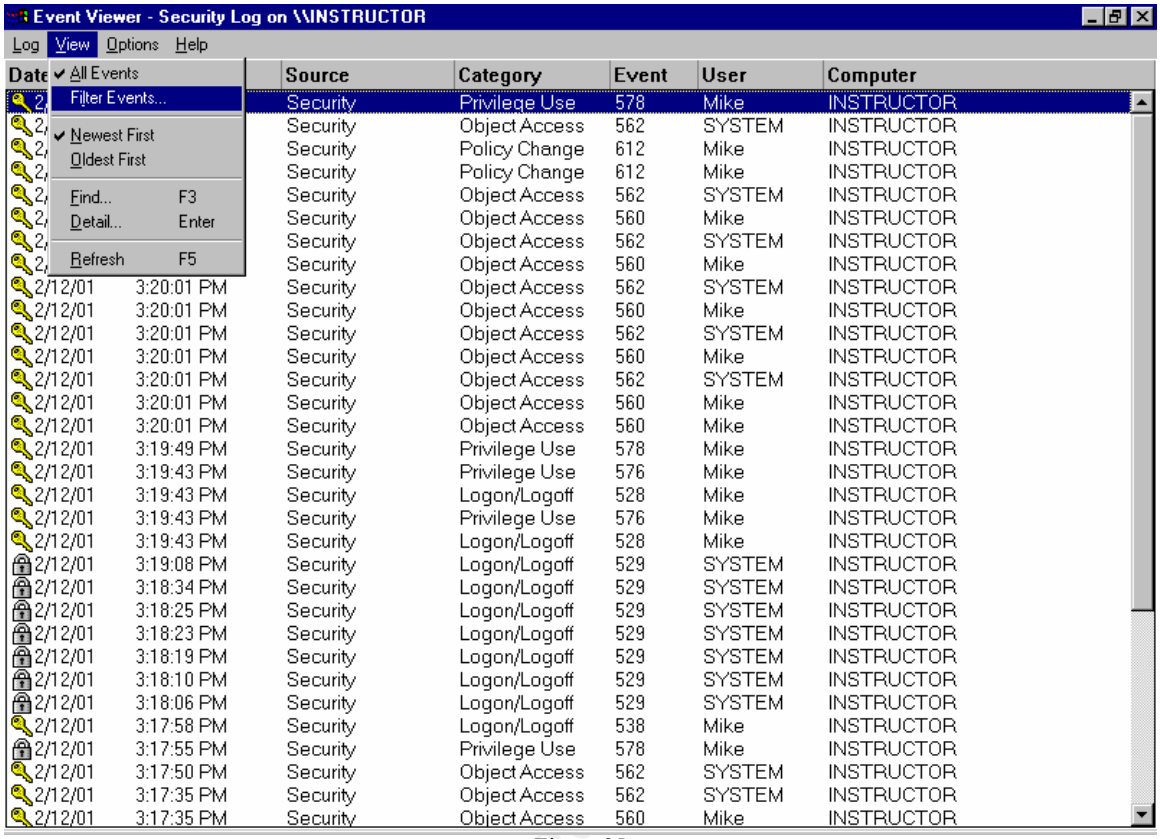


Figure 35

Figure 36 depicts the Filter dialog box. The default dates displayed will be those of the earliest event in the log to the most recent. As I mentioned, for demonstration purposes I generated these logs in a span of just less than 4 minutes, all on the same date. You can see that reflected in the date and time of the filter dialog box.

Had these logs covered multiple days, I could filter for just certain days and times. For example, if I come in Monday morning I could filter for any events that were generated between Friday evening at 5:00:00PM through Monday morning at 8:00:00AM. The filtering mechanism would then display any items that were generated between those dates and times. I would be able to quickly see any event of significance that occurred over the weekend for which I had auditing enabled. This is a very quick and convenient way to view events if time is limited.

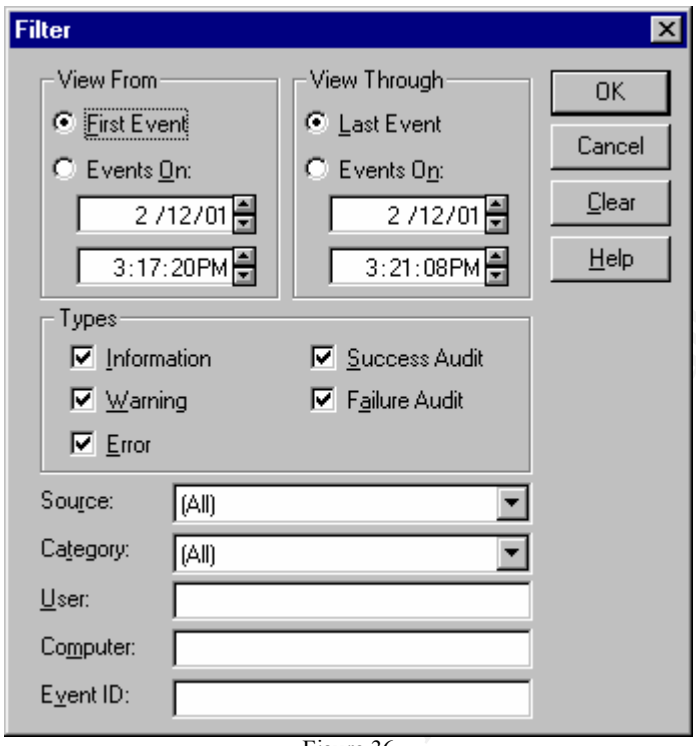


Figure 36

Using my demonstration Security Event Log, I will filter for Failure Audit events only. Figure 37 shows this filter option enabled. In order accomplish this filter, I simply removed the checkmark from all other options under Types and click OK.

Figure 37

Figure 38 below shows the same log as in Figure 35 after filtering for Failure Audit events only. Notice, only events associated with the lock icon are displayed. Again, this log was created for demonstration purposes only. Had it been an actual log there may have been many more events present.

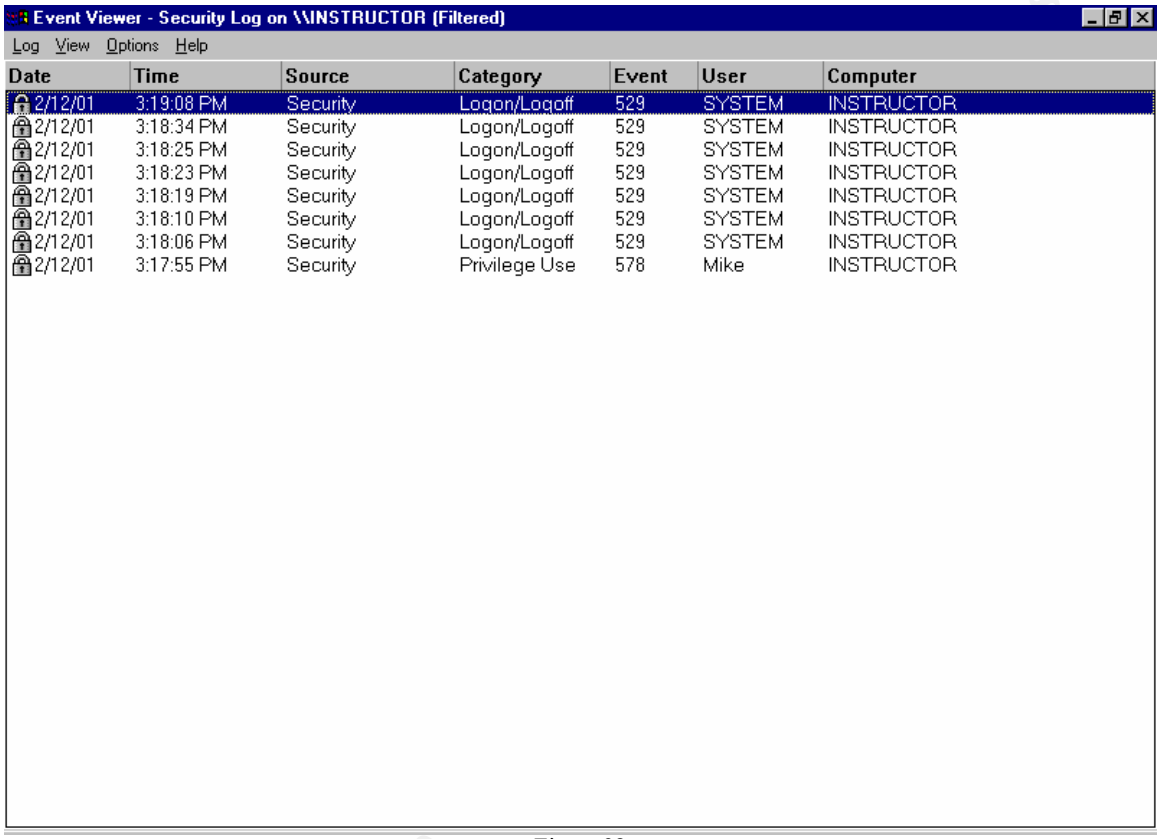


Figure 38

The last topic I cover in this document is items to look for in logs that might raise concern or warrant further investigation. Keep in mind that NT will allow you to filter for any of the events mentioned in that topic.

DumpEvt

There are other options for viewing logs. SomarSoft offers an option in the form of DumpEvt, a tool freely available on the net at http://www.somarsoft.com/.

The following is a description of the tool from the SomarSoft web site:

"**Updated !** SomarSoft's DumpEvt is a Windows NT program to dump the event log in a format suitable for importing into a database. Similar to the DUMPEL utility in the NT resource kit, but without some of the limitations. DumpEvt has been updated to now allow dumping the new Windows 2000 event logs (DNS, File Replication, and Directory Service)"

Ruth Parish offers a good discussion of the DUMPEL Utility in her practical assignment.[15] I will expand upon her information by offering yet another tool for importing logs to a database, DumpEvt.

To use the tool, download and extract the files. Open a Command Prompt and execute dumpevt without options. Figure 39 below is a depiction of what will be displayed.

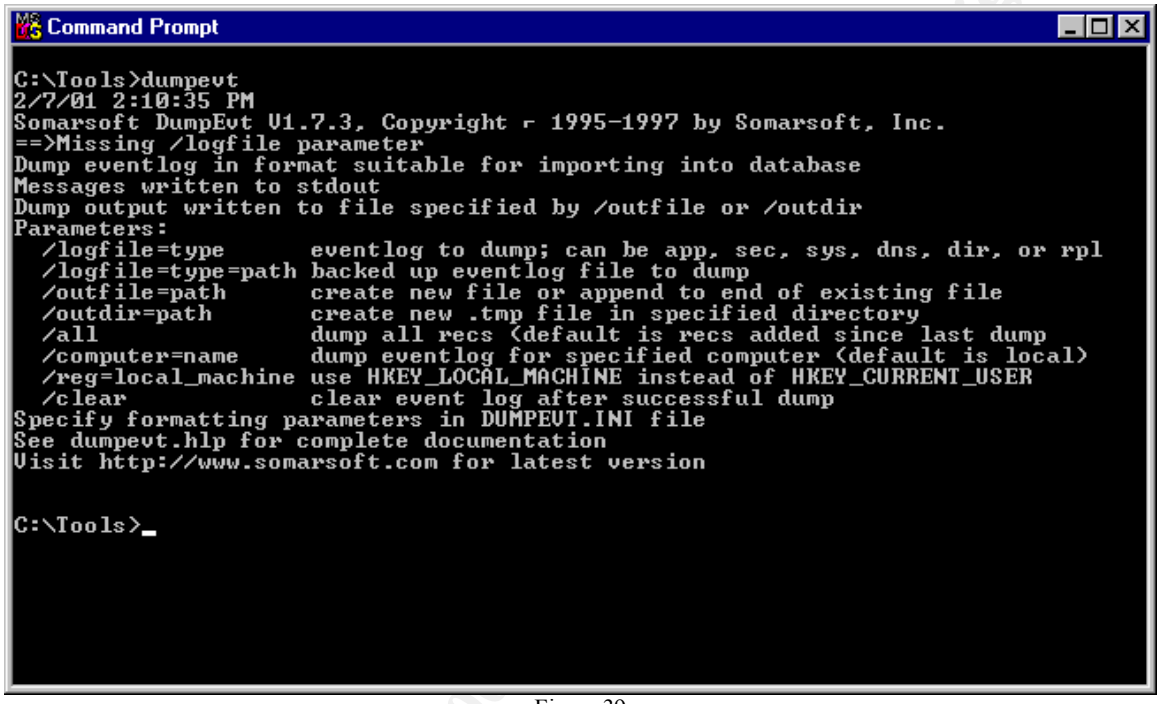


Figure 39

The following screenshot, Figure 40, displays the result of the command to dump the Security Log into a folder I created on my system and named LogDump. DumpEvt will provide feedback as to the execution.

[15] Parish, Ruth Anne "An In-Dept Examination of Event Viewer and Auditing" http://www.s1ans.org/y2k/practical/Ruth_Anne_Parish_GCNT.doc (page 14)

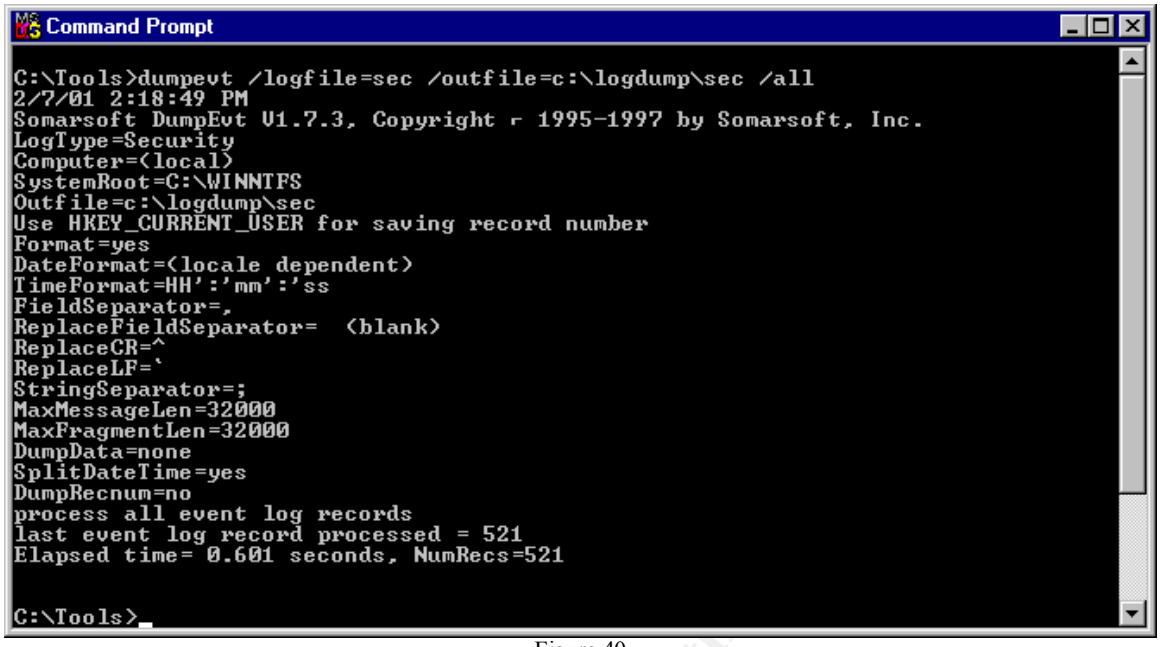


Figure 40

Opening Windows Explorer and the DumpLog Folder, you can see in Figure 41 below, the sec file created by DumpEvt.

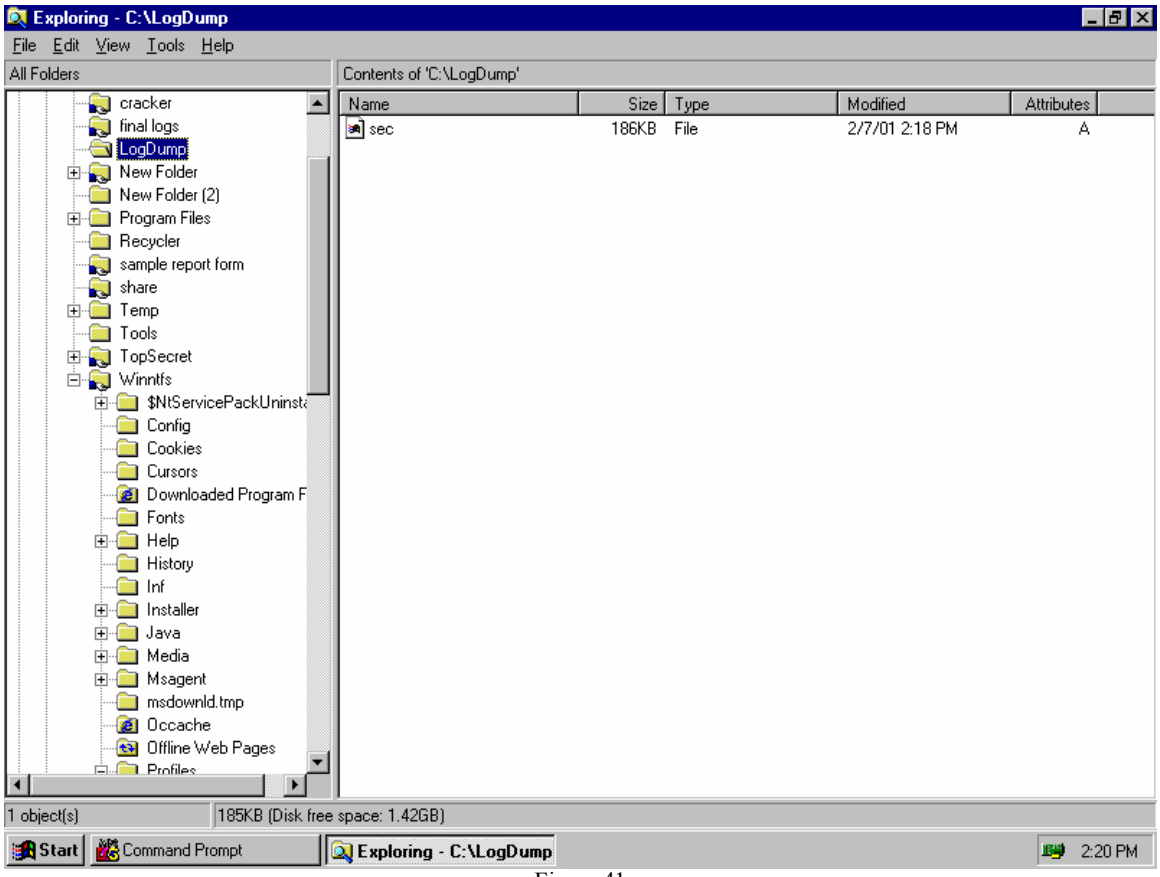


Figure 41

The sec file can now be opened, viewed and manipulated with a variety of applications. Figure 42 below, depicts the sec file opened in an Excel spreadsheet. The tools in Excel can now be used to sort, search, or display the log as desired.

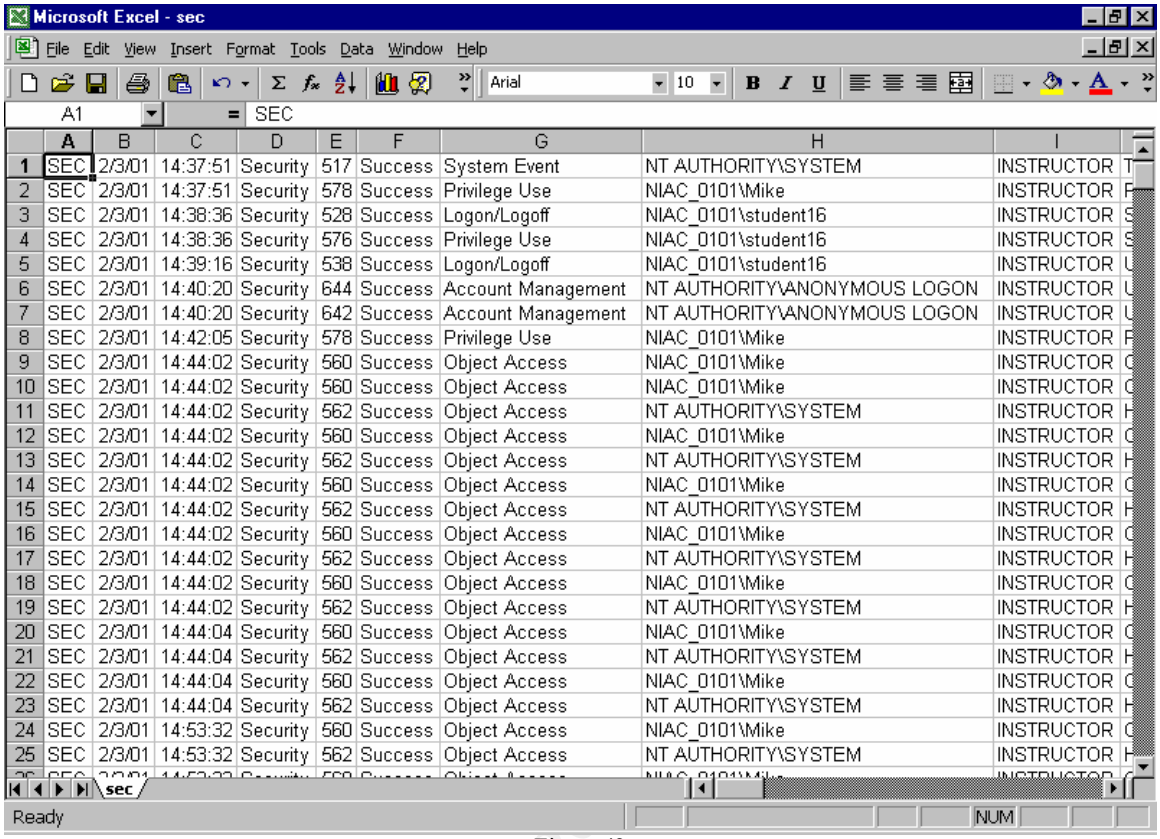


Figure 42

Time Considerations for Saving and Viewing Logs with Event Viewer Application
I will make one final observation concerning viewing saved logs with the Event Viewer Application. First, if logs are to be saved and viewed later with the Event Viewer Application, they must be saved with the .EVT extension. Next, ensure you note the date and time on the machine from which the logs are being saved. Additionally, record the time zone setting. I learned the importance of this the hard way. Luckily there was no damage done as a result of my ignorance. The following screenshots will demonstrate and explain. I will be opening and viewing a log saved previously to a floppy.

To open a saved log file, open Event Viewer and click on Log in the toolbar and Open in the drop-down menu as in Figure 43 below.

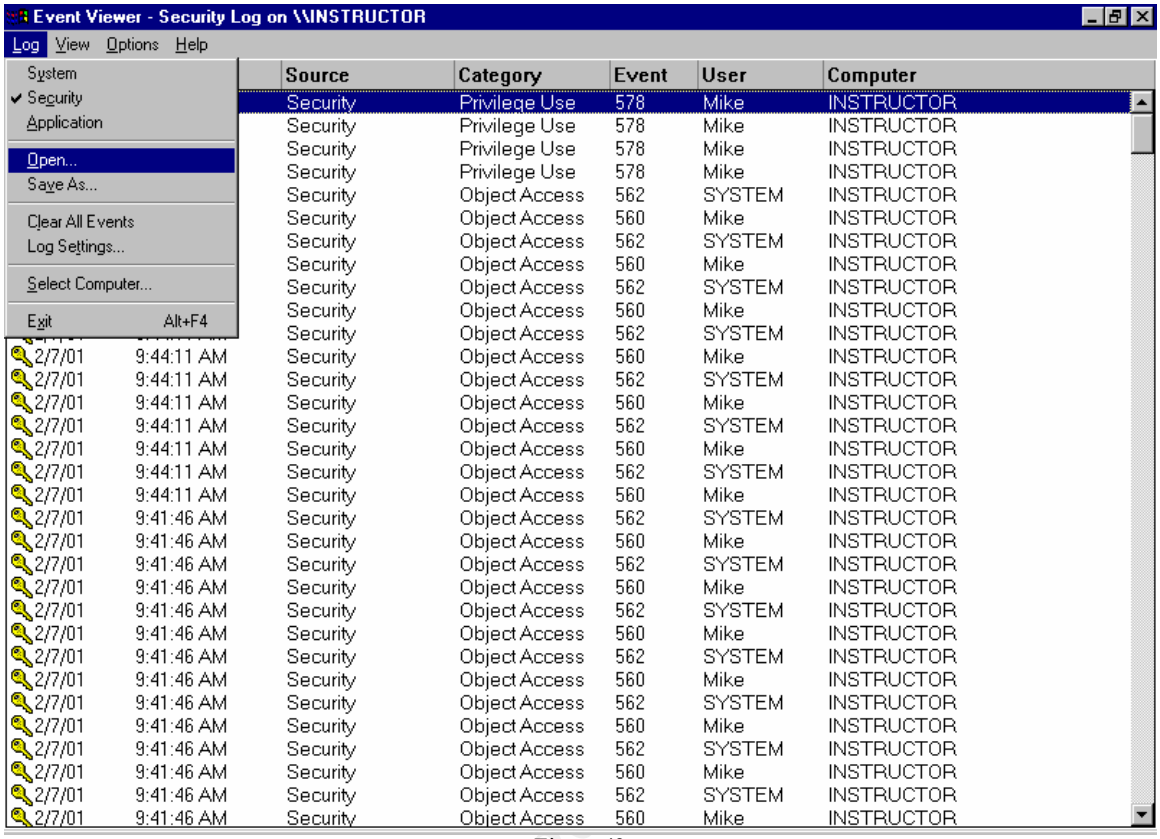


Figure 43

Locate the drive and open the saved log file as demonstrated in Figure 44 below.

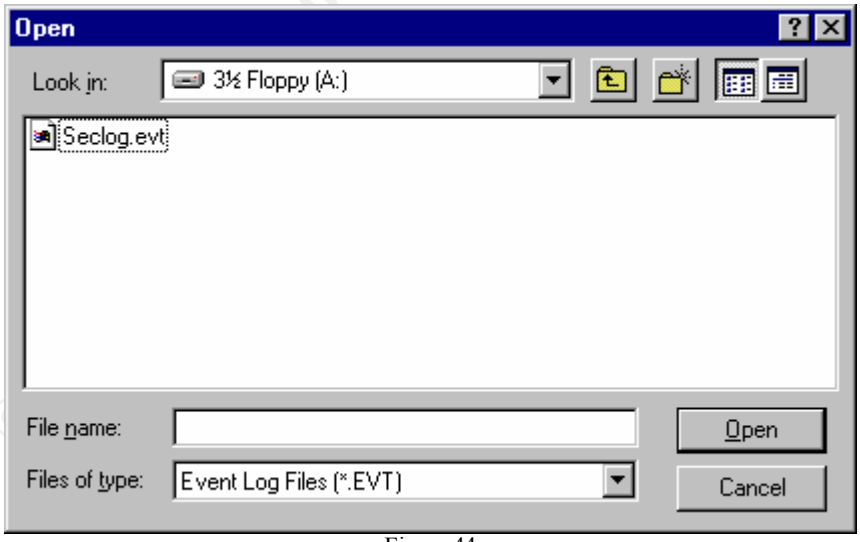


Figure 44

Figure 45 below depicts the next screen displayed. Select the type of log you wish to view. In this example a Security Log file is being opened and thus the radio button is selected for the Security option.

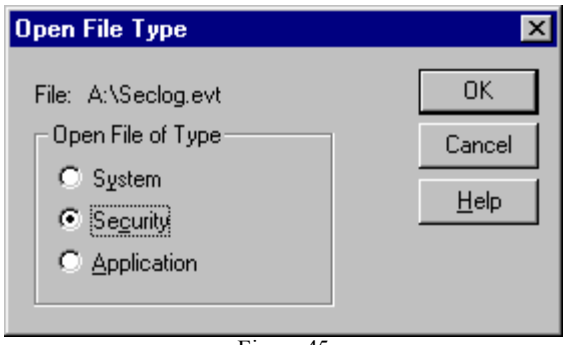
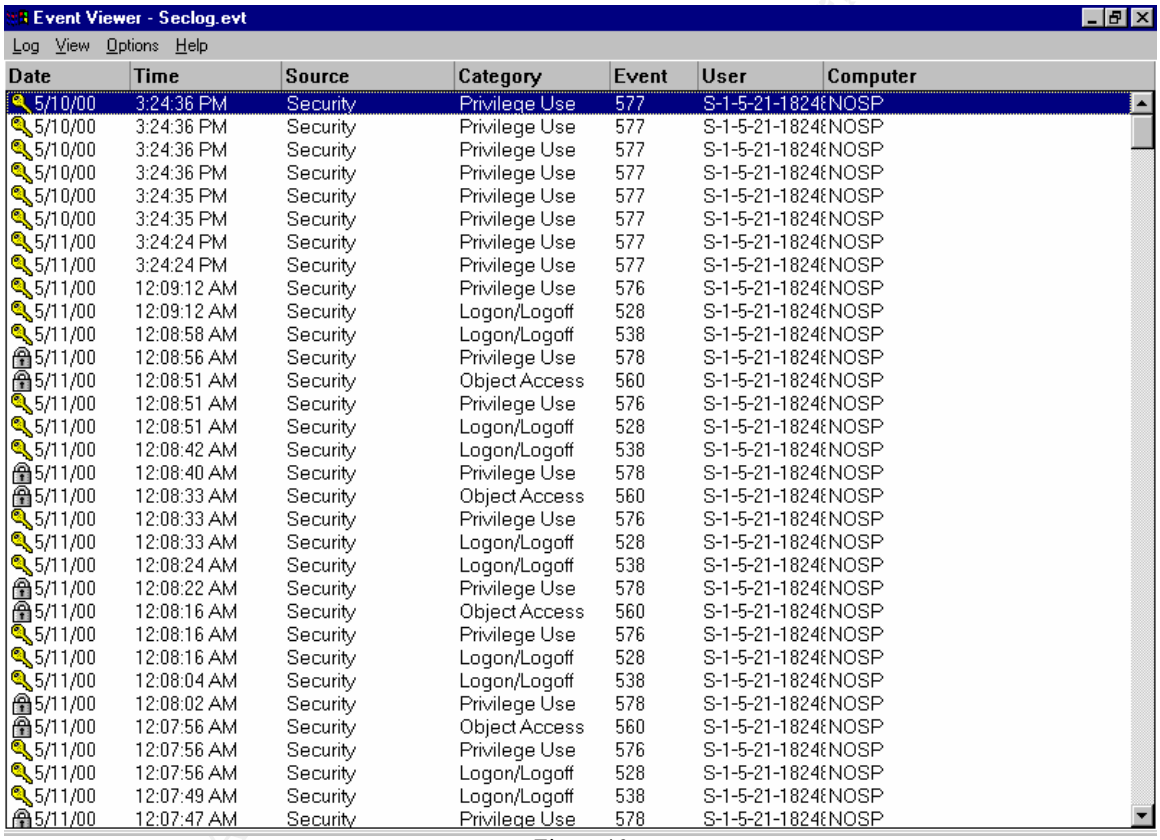


Figure 45

The log file is displayed as in Figure 46 below.



Date	Time	Source	Category	Event	User	Computer
5/10/00	3:24:36 PM	Security	Privilege Use	577	S-1-5-21-1824	NOSP
5/10/00	3:24:36 PM	Security	Privilege Use	577	S-1-5-21-1824	NOSP
5/10/00	3:24:36 PM	Security	Privilege Use	577	S-1-5-21-1824	NOSP
5/10/00	3:24:36 PM	Security	Privilege Use	577	S-1-5-21-1824	NOSP
5/10/00	3:24:35 PM	Security	Privilege Use	577	S-1-5-21-1824	NOSP
5/10/00	3:24:35 PM	Security	Privilege Use	577	S-1-5-21-1824	NOSP
5/11/00	3:24:24 PM	Security	Privilege Use	577	S-1-5-21-1824	NOSP
5/11/00	3:24:24 PM	Security	Privilege Use	577	S-1-5-21-1824	NOSP
5/11/00	12:09:12 AM	Security	Privilege Use	576	S-1-5-21-1824	NOSP
5/11/00	12:09:12 AM	Security	Logon/Logoff	528	S-1-5-21-1824	NOSP
5/11/00	12:08:58 AM	Security	Logon/Logoff	538	S-1-5-21-1824	NOSP
5/11/00	12:08:56 AM	Security	Privilege Use	578	S-1-5-21-1824	NOSP
5/11/00	12:08:51 AM	Security	Object Access	560	S-1-5-21-1824	NOSP
5/11/00	12:08:51 AM	Security	Privilege Use	576	S-1-5-21-1824	NOSP
5/11/00	12:08:51 AM	Security	Logon/Logoff	528	S-1-5-21-1824	NOSP
5/11/00	12:08:42 AM	Security	Logon/Logoff	538	S-1-5-21-1824	NOSP
5/11/00	12:08:40 AM	Security	Privilege Use	578	S-1-5-21-1824	NOSP
5/11/00	12:08:33 AM	Security	Object Access	560	S-1-5-21-1824	NOSP
5/11/00	12:08:33 AM	Security	Privilege Use	576	S-1-5-21-1824	NOSP
5/11/00	12:08:33 AM	Security	Logon/Logoff	528	S-1-5-21-1824	NOSP
5/11/00	12:08:24 AM	Security	Logon/Logoff	538	S-1-5-21-1824	NOSP
5/11/00	12:08:22 AM	Security	Privilege Use	578	S-1-5-21-1824	NOSP
5/11/00	12:08:16 AM	Security	Object Access	560	S-1-5-21-1824	NOSP
5/11/00	12:08:16 AM	Security	Privilege Use	576	S-1-5-21-1824	NOSP
5/11/00	12:08:16 AM	Security	Logon/Logoff	528	S-1-5-21-1824	NOSP
5/11/00	12:08:04 AM	Security	Logon/Logoff	538	S-1-5-21-1824	NOSP
5/11/00	12:08:02 AM	Security	Privilege Use	578	S-1-5-21-1824	NOSP
5/11/00	12:07:56 AM	Security	Object Access	560	S-1-5-21-1824	NOSP
5/11/00	12:07:56 AM	Security	Privilege Use	576	S-1-5-21-1824	NOSP
5/11/00	12:07:56 AM	Security	Logon/Logoff	528	S-1-5-21-1824	NOSP
5/11/00	12:07:49 AM	Security	Logon/Logoff	538	S-1-5-21-1824	NOSP
5/11/00	12:07:47 AM	Security	Privilege Use	578	S-1-5-21-1824	NOSP

Figure 46

Take note of the time for the first item displayed. The log displayed above was saved from a machine on which the time zone was set to the option in Figure 47 below. Notice the Time Zone is (GMT).

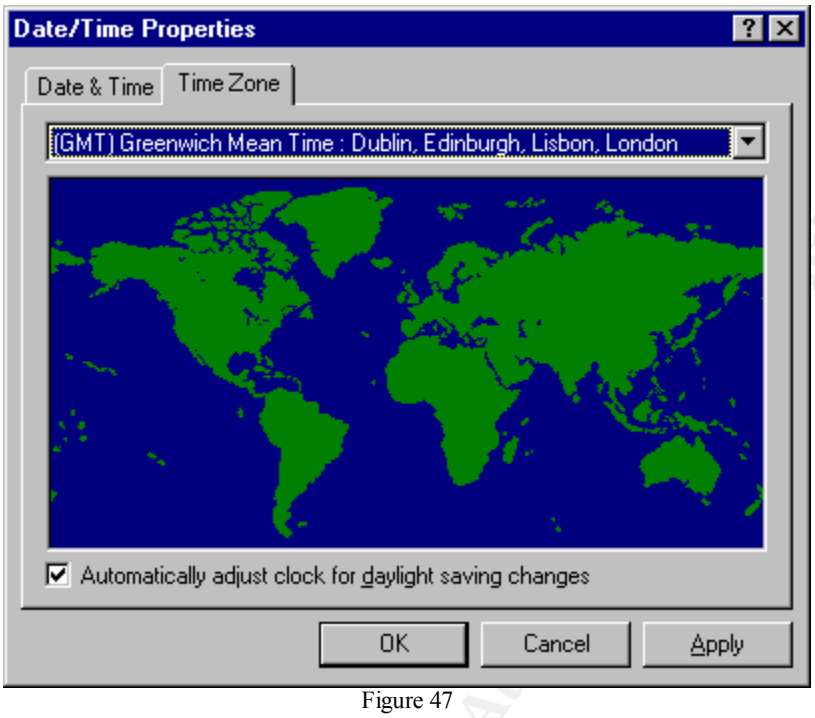


Figure 47

The log in Figure 46 above was opened on a machine with the Time Zone set to the option in Figure 48 below. Does this make a difference? It does make a difference and a very important one depending on how your are using the logs. For example, if they are to be used for legal proceedings, accuracy of time is absolutely imperative.

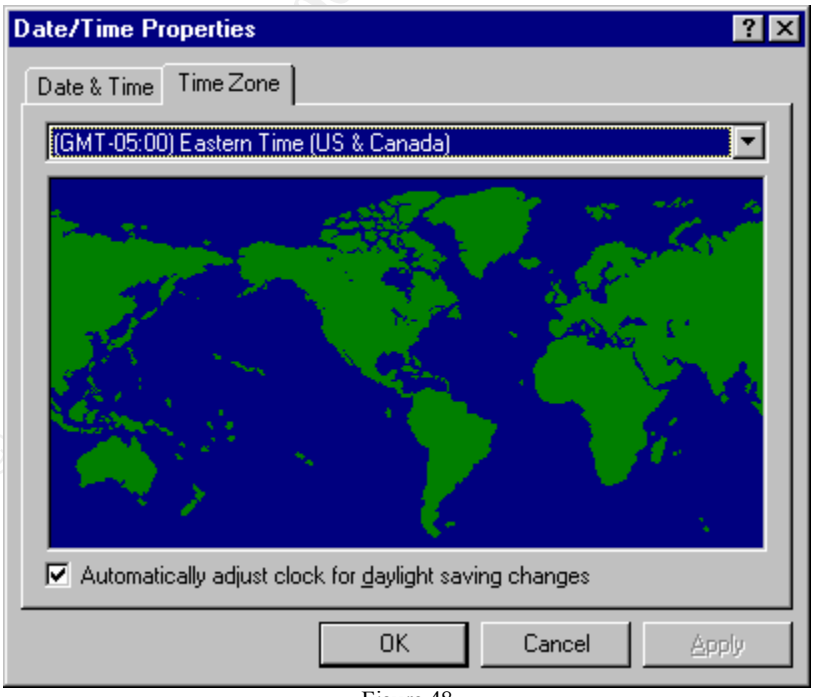


Figure 48

To demonstrate the difference I changed the Date/Time Properties on the viewing system to match the Date/Time on the system from which the logs were taken and when the logs were taken. Figure 49 demonstrates the change. The time zone was changed to that demonstrated in Figure 47 (2 Figures above).

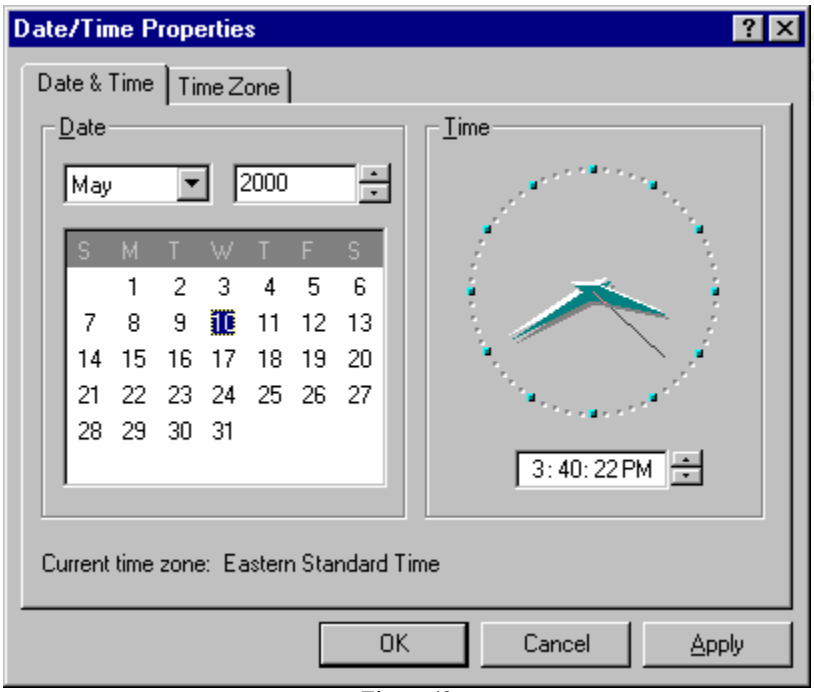


Figure 49

After making the Date/Time changes described directly above I reopened the saved Security Log. The log is shown in Figure 50 below. Notice the difference between the logs in Figure 46 and those shown below. There is a 6 hours difference.

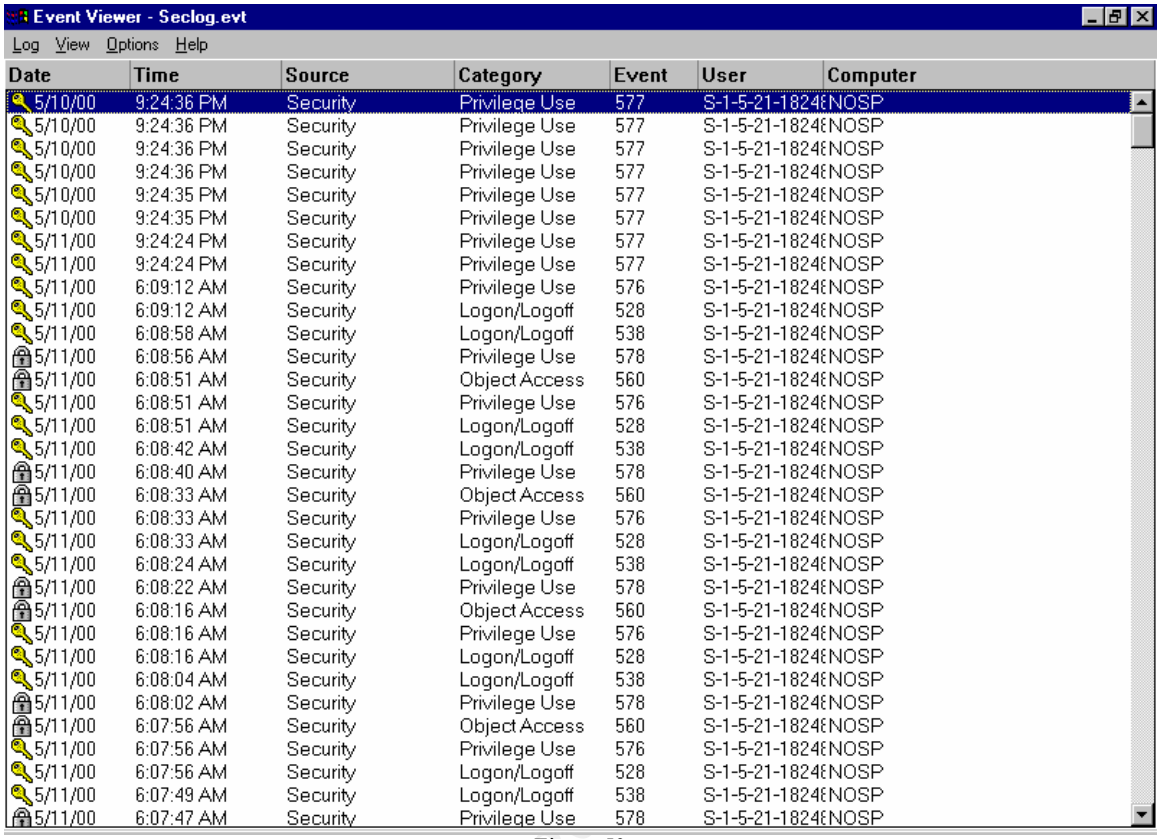


Figure 50

Obviously, this factor must be taken into consideration when viewing saved logs especially if the logs are to be used as evidence in some type of legal proceedings. If logs were saved to a floppy from a machine in California and are being viewed on a machine in New York ensure accuracy of times by ensuring Date/Time Properties on the viewing machine match those of the machine from which the logs originated. This applies to logs saved with the Event Viewer Application using the .EVT extension and then opened and viewed again with Event Viewer.

What to look for in the Security Log

The number of events in the Security Log can easily grow to what appear to be unmanageable figures. Not every Administrator has the luxury of time to devote to analyzing such large log files. However, it may be advisable to scan the logs daily for certain events that might be worth further investigation.

James D. Murray suggests the following:[16]

- Users repeatedly failing to log on
- Users logging onto the system at unusual times, or form unknown remote systems
- Users consistently failing to open files or folders due to insufficient permission

[16] Murray, James D. *Windows NT Event Logging* (O'Reilly & Associates, 1998) page 67.

- Users repeatedly attempting to access system services, but failing due to insufficient privileges

In an article on http://www.securityfocus.com/, Dealing with Windows NT Event Logs Part 2, by Cory L. Scott, he identifies a list of items that might cause concern that include the following:

Event	**ID**
System Restart	512
Audit Log Cleared	517
Unknown Username of Bad Password	529
Account Logon Time Restriction Violation	530
Account Currently Disabled	531
Account Has Expired	532
User Not Allowed To Logon	533
Logon Type Restricted	534
Password Expired	535
Unsuccessful Logon	537
User Right Assigned	608
User Right Removed	609
New Trusted Domain	610
Removing Trusted Domain	611
Audit Policy Change	612
User Account Created	624
Change Password Attempt	627
User Account Deleted	630
Global Group Member Added	632
Local Group Member Added	636
User Account Changed	642
Domain Policy Changed	643

Auditing can seem a daunting and overwhelming task at times. However, it is a necessary task. Thanks to SANS for providing a platform for spreading the knowledge on how best to accomplish the job. Thanks also to all SANS students for sharing your knowledge and expertise.

References

Carboni, Christopher
http://www.sans.org/y2k/practical/Chris_Carboni.doc

Gabert, Howard F. "Using Event Logs to Audit Windows NT4"
http://www.sans.org/y2k/practical/Howard_Gabert.doc

Golias, Martin. GCNT Practical Assignment. The SANS Institute.
http://www.sans.org/y2k/practical/Martin_Golias.doc

Hadfield, Lee; Hatter, Dave; Bixler, Dave. *Windows NT Sever 4 Security Handbook*
Que® Corporation, 1997.

Murray, James D. *Windows NT Event Logging*
O'Reilly & Associates Inc., September 1998. Sebastopol, CA.

Otis, Brig, SANS Practical, Track 5: Windows Security Monterey, 2000
http://www.sans.org/y2k/practical/brigs_otis GCNT.doc

Parish, Ruth Anne "An In-Dept Examination of Event Viewer and Auditing"
http://www.s1ans.org/y2k/practical/Ruth_Anne_Parish_GCNT.doc

Payne, Jeff "Practical Assignment For SANS Security Monterey 2000"
http://www.sans.org/giactc/gcnt.htm

Saxinger, Justin "Essential Steps for Securing a Windows NT 4 Server"
http://www.sans.org/y2k/practical/Justin_Saxinger_GCNT.doc

Scambray, Joel; McClure, Stuart; Kurtz, George. *Hacking Exposed*, Second Edition
Network Security Secrets & Solutions. Osborne/McGraw Hill, 2001.

Scott, Cory L. "Dealing with Windows NT Event Logs Part 2"
http://www.securityfocus.com/

Toy, Steven "Centralized Auditing of a Windows NT Computer"
http://www.sans.org/y2k/practical/Steven_Toy.doc

Last Updated: July 22nd, 2017

Upcoming Training

SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**