GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

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

WINDOWS NT AUDITING
SECURING YOUR NETWORK

SANS GCNT PRACTICAL ASSIGNMENT
MAY 2001
KATHRYN SALYERS

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

TABLE OF CONTENTS

	Page
Introduction	4
Part I – Using Windows NT Auditing	4
Why Audit	4
How Does Auditing Work	4
Event Categories	4
Event Viewer	5
Managing Auditing	6
Step 1 – Select Categories to Audit	6
Step 2 – Select File and Object Access Auditing	8
Step 3 – Configure Log File Settings	9
Part II – Log File and Events	11
Maximum Log Size	11
Event Log Wrapping	11
Archiving Data	12
Interpreting Events	13
Intrusion Detection Systems	15
Part III – Maintain Audit and Log Settings with Security Configuration Manager	15
Customizing Templates	15
Performing a Security Analysis	17
Bringing a System Into Compliance	18
Part IV – Common Auditing Practices	20
Defining an Audit Policy	20
Recommended Auditing Practices and Associated Event IDs	21
Conclusion	30
References	32

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

TABLE OF FIGURES

	Page
Figure 1: Event Categories	4
Figure 2: Event Viewer/View/Log	5
Figure 3: The User Manager Utility/Audit Policy Events	7
Figure 4: Microsoft Management Console/Security Configuration Editor	7
Figure 5: Audit Policy Changes in Security Configuration Editor	8
Figure 6: Using Windows Explorer to Set Directory Auditing	8
Figure 7: Using SCM to Set Directory Auditing	9
Figure 8: Using Event Viewer to Configure Log Settings	10
Figure 9: Using SCE to Configure and Maintain Log Settings	10
Figure 10: Event Viewer/Save As	12
Figure 11: The DUMPEL.EXE Utility	12
Figure 12: The AT Command	13
Figure 13: Event Detail/New User	13
Figure 14: Event Filter	14
Figure 15: Customizing a Template	16
Figure 16: Importing Customized Template into Database	16
Figure 17: Using the SCE Utility to Perform a Security Analysis	17
Figure 18: Security Analysis Results Indicating Deviations from Standard Policy	18
Figure 19: The *Configure System Now* Option	19
Figure 20: SECEDIT.EXE	20
Figure 21: Logon/Logoff Events – Corresponding Ids 528 and 538	23
Figure 22: Logon Type 7 – Unlocking a Workstation	23
Figure 23: Event Detail Policy Change – turning off all logging	24
Figure 24: Event ID 560 – Object Access, System as Primary User	27
Figure 25: Event ID 564 Object Delete Handle ID	28
Figure 26: Event ID 560 Cross-Referencing Handle ID	29
Figure 27: Process Tracking – Creating a New Process	30

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Introduction

A vital part of securing Windows NT networks includes utilizing the NT Audit feature and regularly monitoring the log files. Auditing provides several benefits. It serves to ensure proper access permissions to legitimate users, provides a record of authorized and/or unauthorized network activities, and can prevent further intrusion.

This paper provides 1) a general overview regarding why, how and when to use Windows NT Auditing; 2) how to manage and interpret log files; 3) a reference for utilizing the Security Configuration Manager to ensure auditing configurations are consistent in an environment in which there are several administrators; and 4) a description of recommended auditing practices.

Part I
Using Windows NT Auditing

Why Audit

Auditing events is an essential aspect of securing NT networks. Auditing ensures accountability for the actions of network administrators and users. Auditing allows an administrator to verify that NTFS and share permissions are set correctly. And auditing can identify system penetrations.

How Does Auditing Work

<u>Event Categories</u>
The NT administrator selects certain security events to write to a security log. These events are grouped into seven categories. Enabling Auditing requires that for seven categories you select to audit success, failure, both or neither.

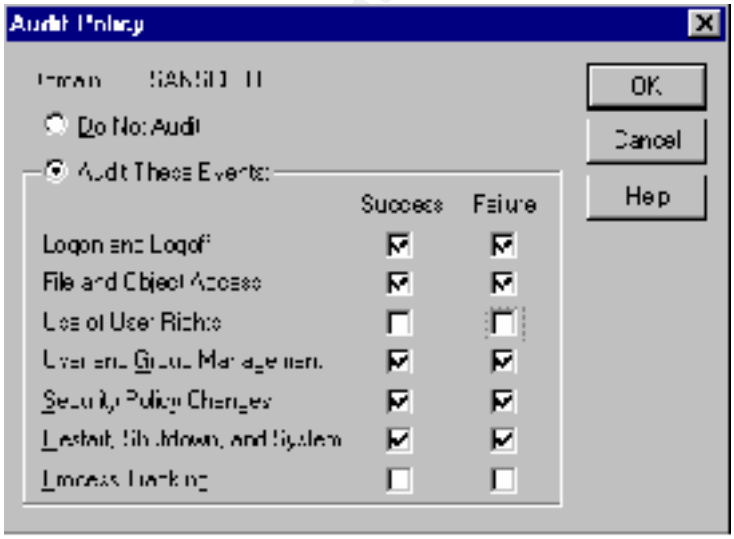

Figure 1: Event Categories

User Manager and the Event Viewer use slightly different names for the seven categories. Listed are the Category Names:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

In User Manager …	In Event Viewer …
Logon and Logoff	Logon/Logoff
File and Object Access	Object Access
Use of User Rights	Privilege Use
User and Group Management	Account Management
Security Policy Changes	Policy Change
Process Tracking	Detailed Tracking
Restart, Shutdown, and System	System Event

The seven event categories are described as follows:

Logon and Logoff
This selection records primary and secondary logons and logoffs (a secondary logon is a logon from another workstation to a network share on local machine).

File and Object Access
This selection records access by programs to files, directories, or other objects.

Use of User Rights
This selection records actions by programs that require a Right such as Add Workstations to Domain.

User and Group Management
This selection records adding, changing, or deleting accounts or groups.

Security Policy Changes
This selection records changes in the Auditing and Rights Policies.

Restart, Shutdown, System
An event is recorded if a system is restarted or shutdown.

Process Tracking
Events are recorded as NT manages programs and other internal attributes.

<u>Event Viewer</u>

The Event Viewer allows the security administrator to view and manage various logs. The Security Log records events related to the seven categories described above.

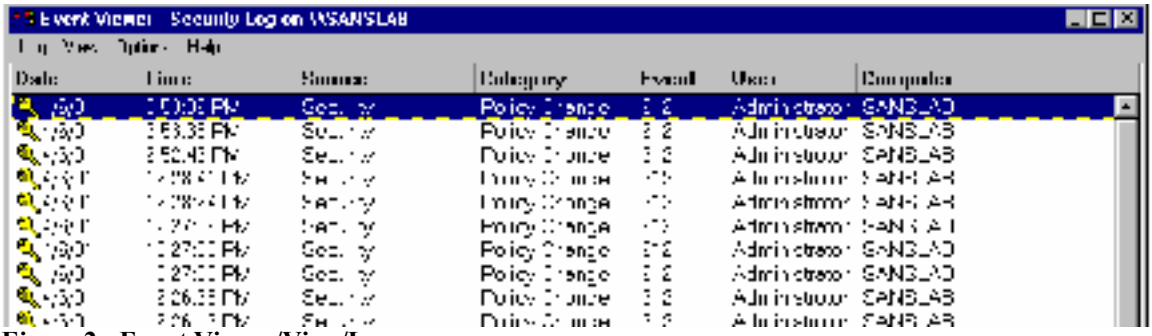

Figure 2: Event Viewer/View/Log

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Each row is an event. Each event includes the following information:

Success or Failure (Lock or Key icon)
A "lock" icon is recorded for unsuccessful events and a "key" icon is recorded for successful events.

Time
The time the event occurred.

Source
NT modules – The Security Log will indicate "Security" in this column

Category
This is one of the seven categories

Event
This is the Event ID, a number unique to each kind of event. For example, Event ID 562 indicates successful access to a file.

User
The logon id of the user performing the activity

Computer
The workstation on which the event occurred.

Managing Auditing

There are several utilities available to configure, monitor and manage auditing and event logging including User Manager, Event Viewer, Windows Explorer and Security Configuration Editor.

Step 1 - configure auditing to enable the auditing feature by selecting the categories/events to audit.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The User Manager utility

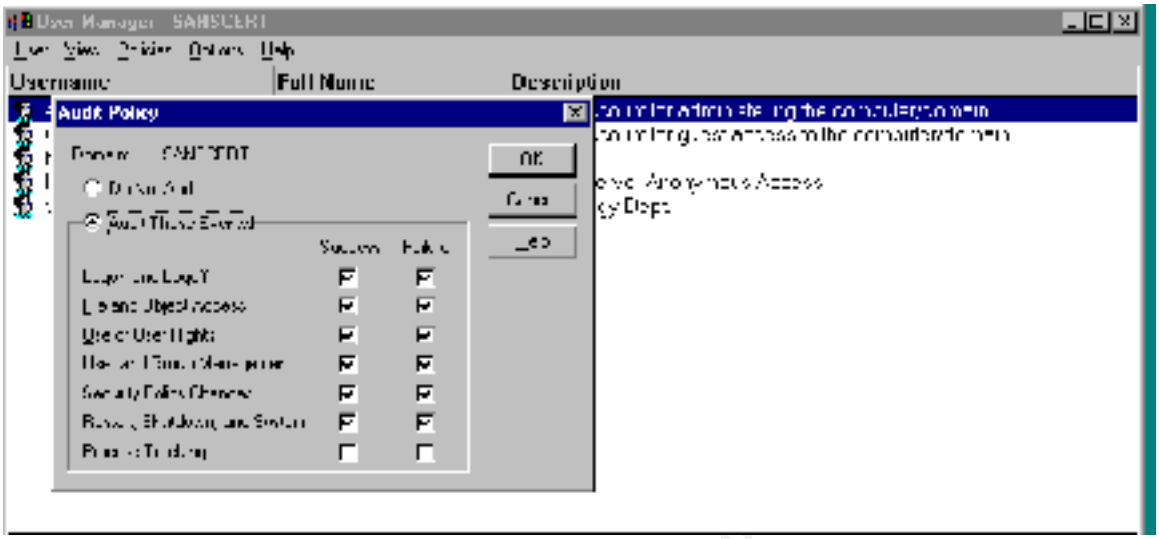

Figure 3: The User Manager Utility/Audit Policy Events

The Microsoft Management Console utility

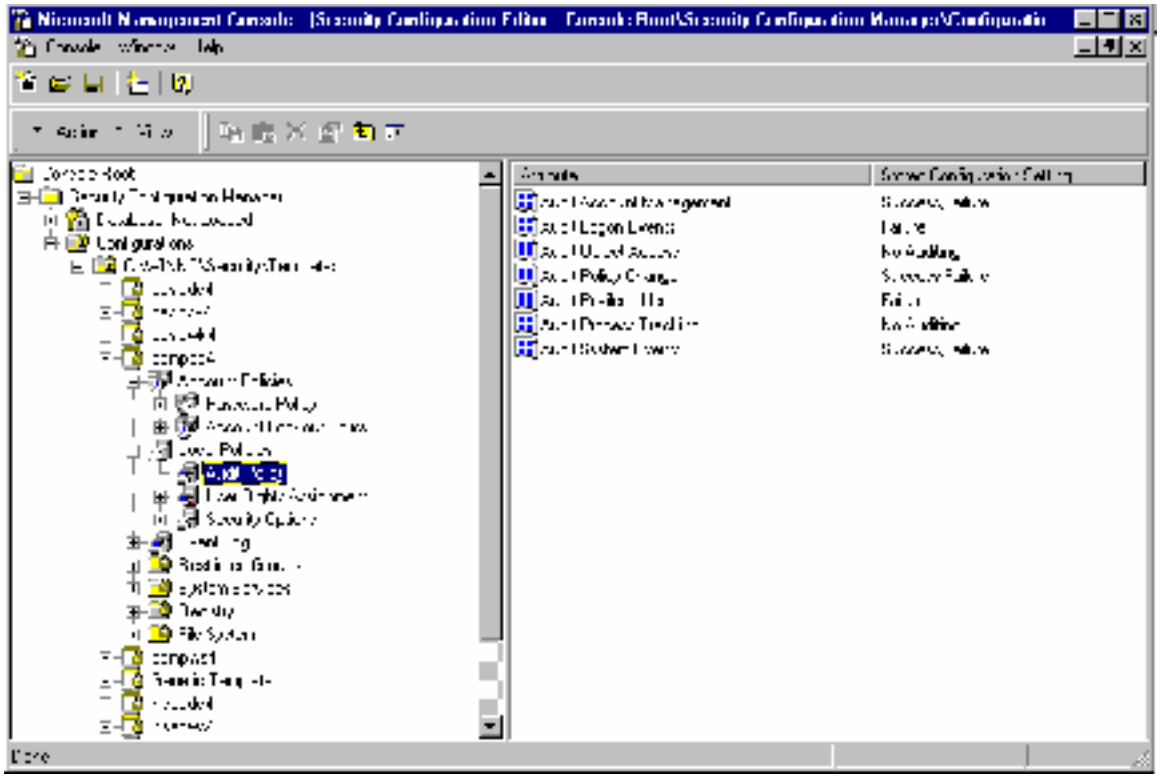

Figure 4: Microsoft Management Console/Security Configuration Editor

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

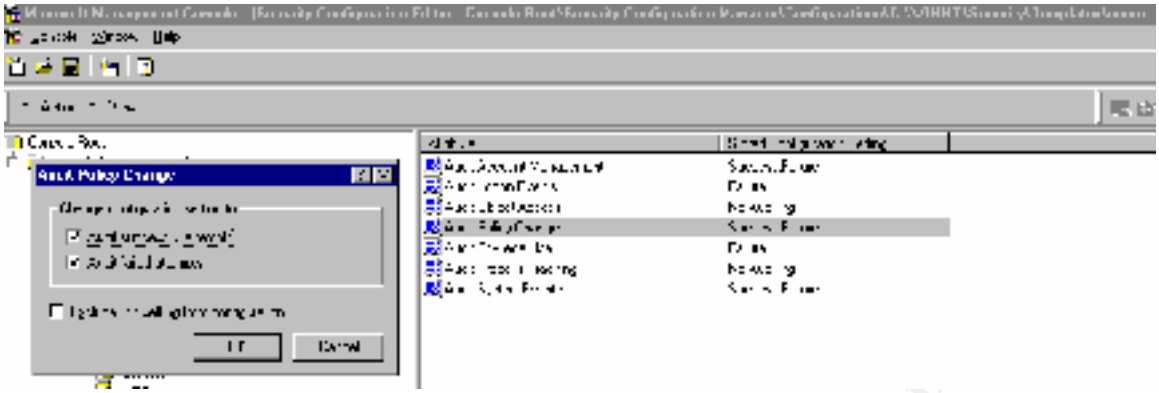

Figure 5: Audit Policy Changes in Security Configuration Editor

Step 2 – if Audit Object Access event is selected for auditing, select directories and files to audit and add user accounts to monitor.

Windows Explorer

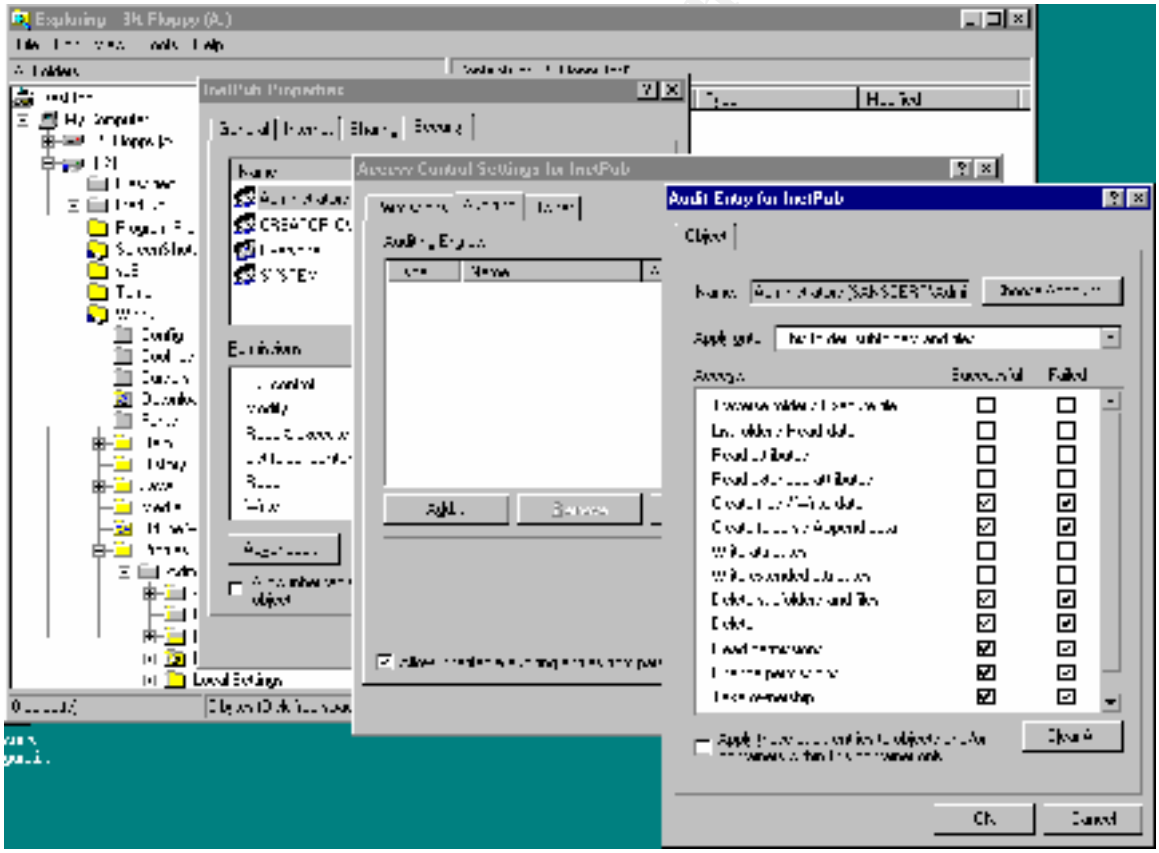

Figure 6: Using Windows Explorer to Set Directory Auditing for the Administrator Account

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

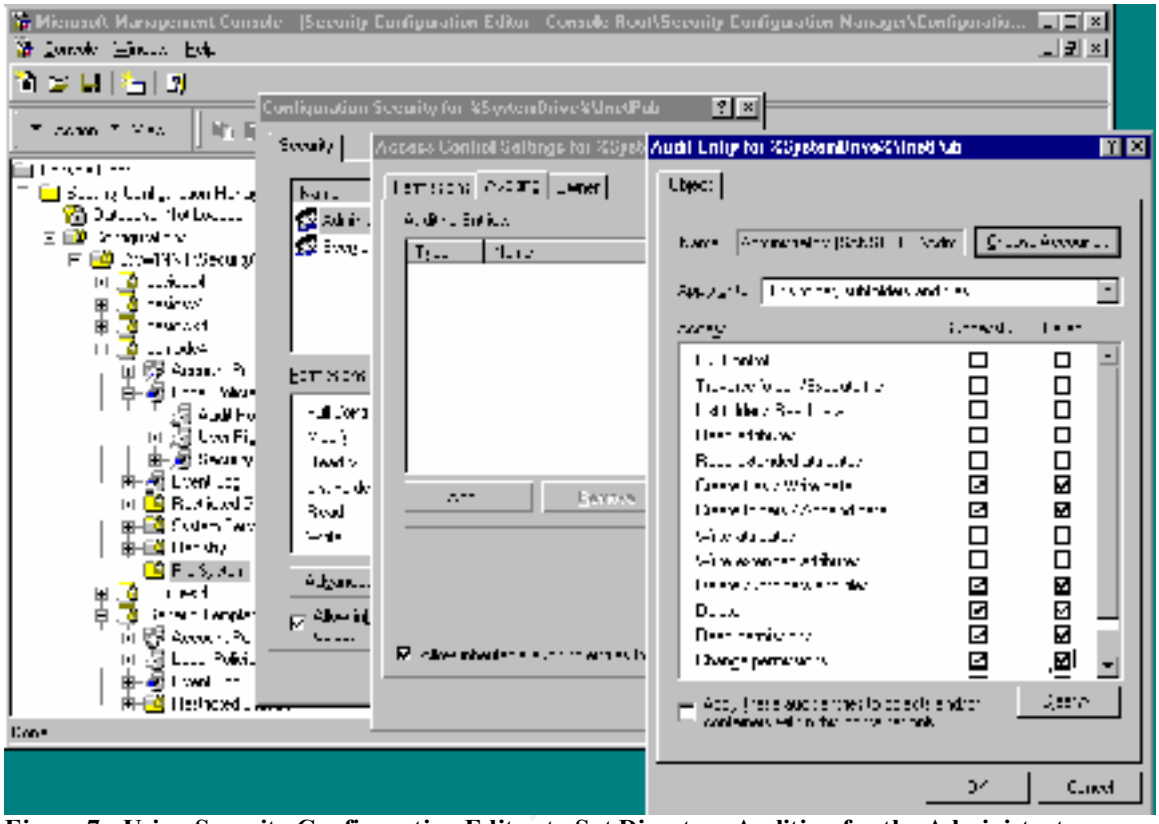

Figure 7: Using Security Configuration Editor to Set Directory Auditing for the Administrator Account

<u>Step 3</u> – Configure Log File Settings

Log files are saved on a hard drive. It is important to consider disk space as the log files can consume available space, and if located on the system partition, affect the performance of the system.

Event log settings are configured for maximum log size and event log wrapping. Keeping this information private deters intruders from using this information to try to fill the log. Be aware that changes to the maximum event-log size do not take effect until after you clear the log.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Event Viewer

Figure 8: Using Event Viewer to Configure Log Settings

Microsoft Management Console

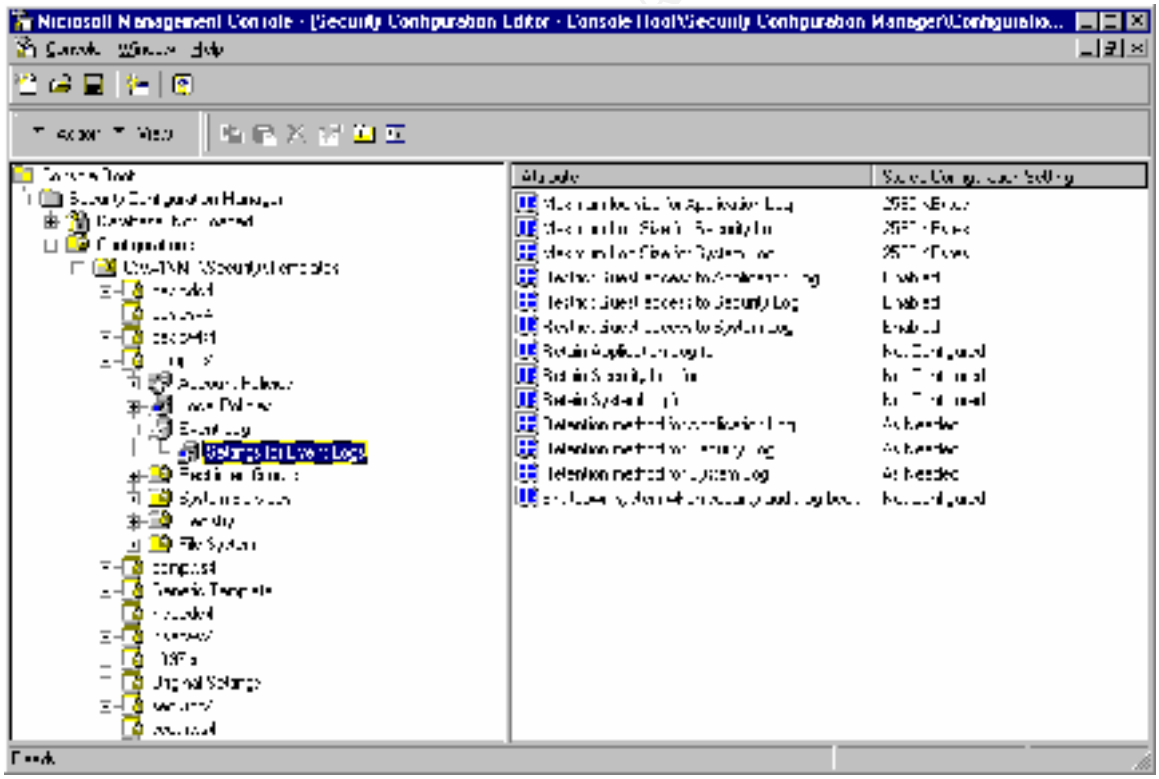

Figure 9: Using Microsoft Management Console to Configure and Maintain Log Settings

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Part II
Log Files and Events

Information in the log files can identify violators who made it past your previous layers of security, including authentication and access control policies. An audit trail lets you detect suspicious activity by monitoring users' actions even when they have obtained administrative access rights. Maximizing the benefits a security log can provide includes managing the size of the security log, preserving the data, and interpreting the events.

NT records events in the security log and the log grows until it reaches its maximum log size. Correctly configuring the log file settings and properly archiving data ensures that critical logging events are not lost.

Maximum Log Size

Determining the optimal setting for the Maximum Log Size depends on available disk space; the activity on your system; the event categories you enable for auditing; and especially the level of object auditing you are using. Because the Security Log is so important, it should have a relatively large size and, in combination with wrapping and archiving, provide for a continuous audit trail. Identifying the proper file size includes adjusting and fine-tuning the file size based on normal activity.

Event Log Wrapping

You can select *Overwrite Events as Needed*, discarding the oldest events as NT records new events. The setting *Overwrite Events Older than X Days* records events until the log is full. NT will then discard events older than the specified number of days as needed to allow space for new events. If the log becomes full of events younger than the specified number of days, NT stops recording events until some events expire. Choosing the setting *Do Not Overwrite Events (Clear Log Manually)* results in NT recording events until the log is full. No new events are recorded until the log is manually cleared.

Each of these setting provides an attacker with an opportunity to manipulate the data and cover their tracks. The *Overwriting Events as Needed* setting allows an attacker to fill the log with normal events, effectively flushing the log file of critical events related to their activities. Both the *Overwrite Events Older than X Days* and the *Do Not Overwrite Events* settings will stop writing new events to the log under certain conditions, causing loss of data. The security administrator can use the CrashOnAuditFail registry setting to cause the server to shut down when the security log is not logging events. However, until the server is rebooted its services are unavailable to users. An attacker may exploit this setting to cause a Denial of Service attack by filling up the log to intentionally crash the system.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Archiving Data

Overwriting events can cause the loss of critical logging information. Saving and archiving the logs prevent lost data when the maximum log size is reached. Unauthorized activities can occur over a period of time before you are aware of them. Keeping the data provides information required when building a case against intruders.

Event Viewer provides an option to save log files.

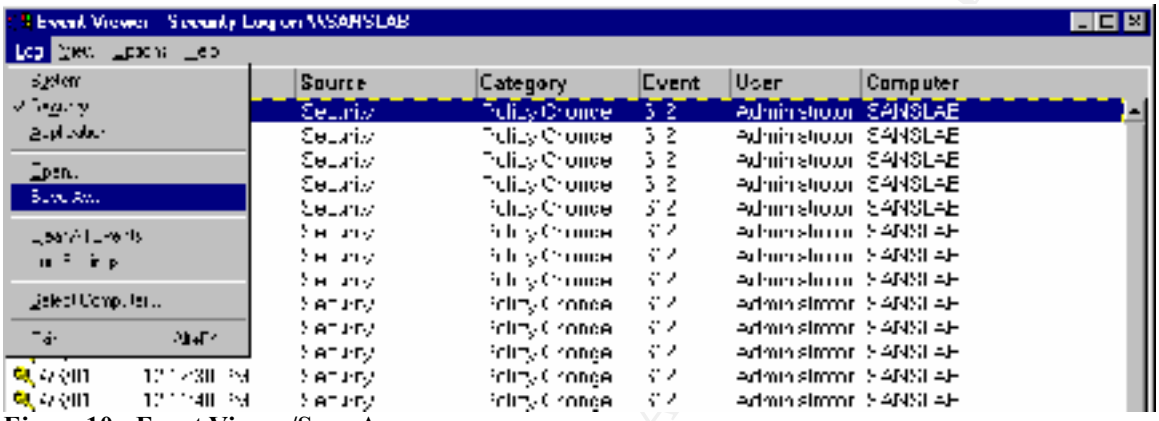

Figure 10: Event Viewer/Save As

Properly preserving the log file data includes configuring a batch file routine to automatically save the log files. The *Microsoft Windows NT Server 4.0 Resource Kit* provides the Dumpel utility to automate this process. This command-line utility can be used to dump an event log into a tab-separated text file. To use Dump Event Log, type dumpel with the appropriate switches at the command prompt.

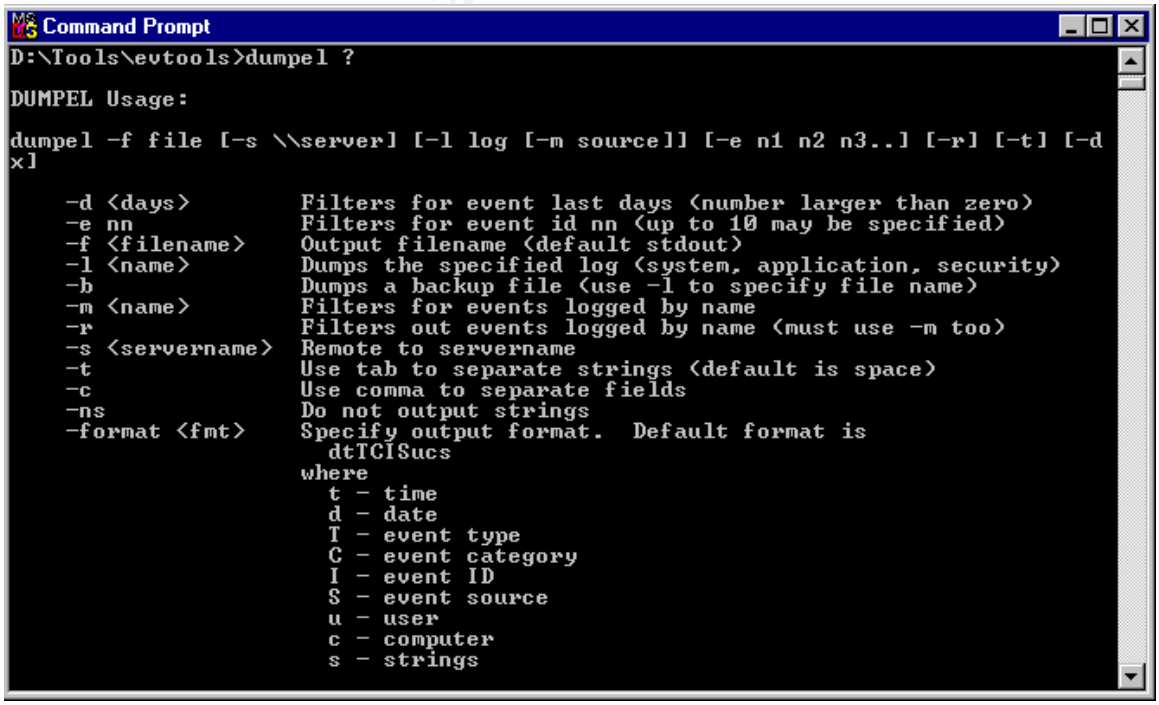

Figure 11: DUMPEL.EXE

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Use the NT Schedule service, the AT command, to execute the dumpel command daily.

```
Command Prompt
AT [\\computername] [ [id] [/DELETE] | /DELETE [/YES]]
AT [\\computername] time [/INTERACTIVE]
    [ /EVERY:date[,...] | /NEXT:date[,...]] "command"

\\computername      Specifies a remote computer. Commands are scheduled on the
                    local computer if this parameter is omitted.
id                  Is an identification number assigned to a scheduled
                    command.
/delete             Cancels a scheduled command. If id is omitted, all the
                    scheduled commands on the computer are canceled.
/yes                Used with cancel all jobs command when no further
                    confirmation is desired.
time                Specifies the time when command is to run.
/interactive        Allows the job to interact with the desktop of the user
                    who is logged on at the time the job runs.
/every:date[,...]   Runs the command on each specified day(s) of the week or
                    month. If date is omitted, the current day of the month
                    is assumed.
/next:date[,...]    Runs the specified command on the next occurrence of the
                    day (for example, next Thursday).  If date is omitted, the
                    current day of the month is assumed.
"command"           Is the Windows NT command, or batch program to be run.

K:\home\kathryns>_
```

Figure 12: AT command to automate event log dumps

The nightly tape backup routine then archives the file to tape preserving the data.

Interpreting Events

Monitoring the log files includes viewing and interpreting the event details. The following example is an event detail logged after creating a new user account.

Figure 13: Event Detail/New User

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A reference for a complete list of security event descriptions is found in the Microsoft article "Security Event Descriptions" at http://support.microsoft.com/support/kb/articles/q174/0/74.asp.

You can configure Event Manager to filter events on criteria such as user, event id, or specific dates.

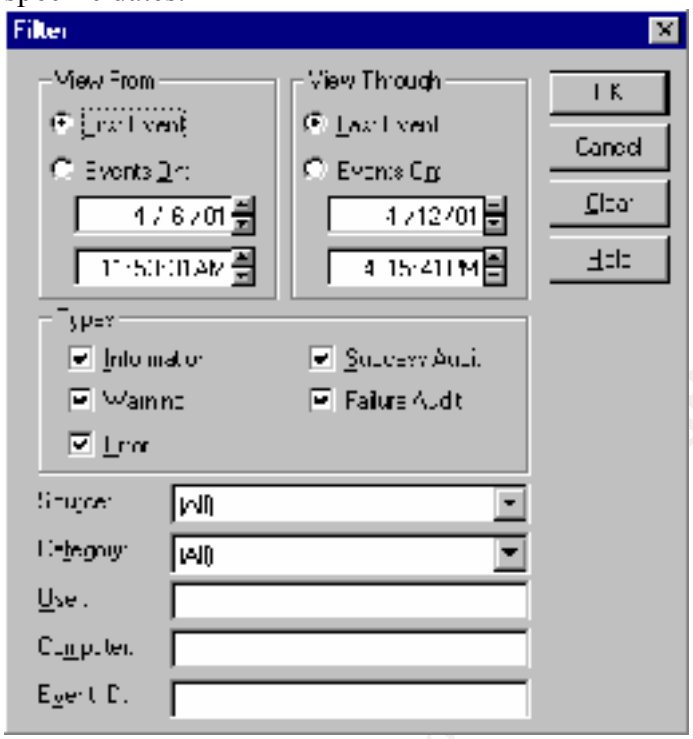

Figure 14: Event Filter

Filtering events is useful for sifting through valid events in an effort to locate events that may indicate unauthorized activity. Just as the Dumpel utility is useful in saving event logs, it can also be used to filter events.

For example, to identify logon failures on a domain controller create a batch file to query the security event log and filter to find the logon failure events as in the following example:

```
Dumpel.exe -s pdcname -l security -m security -e 529  >
dirname\event529.txt
```

This will append all Event 529s to the event 529.txt file for review to identify log on failures on the PDC.

```
   Event ID: 529
       Type: Failure Audit
Description: Logon Failure:
             Reason: Unknown user name or bad password
             User Name: %1              Domain: %2
             Logon Type: %3             Logon Process: %4
             Authentication Package: %5 Workstation Name: %6
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Invalid logon events indicate that a user is entering the wrong password or an unauthorized individual is trying to gain access to the network.

Intrusion Detection Systems

Intrusion Detection Systems collect and analyze data from systems, and attempt to discover statistical patterns of intrusion by comparing the activity to information in a database. The information in the database includes patterns related to known attacks, as well as patterns learned from normal behavior of systems.

Intrusion Detection Systems provide an automated method for collecting and analyzing log file data, comparing network traffic and host log entries to the known and likely methods of attackers. Suspicious activities trigger administrator alarms and send alerts.

A popular product for intrusion detection is *Real Secure* (http://www.iss.net). This product includes Secure Log Manager, a software application designed to meet the requirements of managing system audit logs. On each managed Windows system, the Secure Log Manager Agent monitors the size of all event logs. If a log reaches a set threshold/trigger condition the log is transferred to the Secure Log Manager Collector on a central management platform (the transfer of logs can also be triggered by time). The data may then be used for later analysis or investigation.

Part III
Ensuring audit policy settings, directory and file access logging and event log settings remain in compliance with security policy

The Microsoft Management Console provides a snap-in utility, the Security Configuration Editor, highly useful for configuring and maintaining audit and logging policies. A brief overview of the use of the Security Configuration Editor is provided here. For a step-by-step guide see Lisa Yeo's article "Configuring and Auditing Windows NT With Security Configuration Manager" at http://www.sans.org/giactc/gcnt.htm.

Customizing Templates

The Security Configuration Editor provides templates with standard security settings for workstations, servers, and domain controllers at three basic security levels—default, somewhat secure, and highly secure. These templates can be customized to meet an organization's needs.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

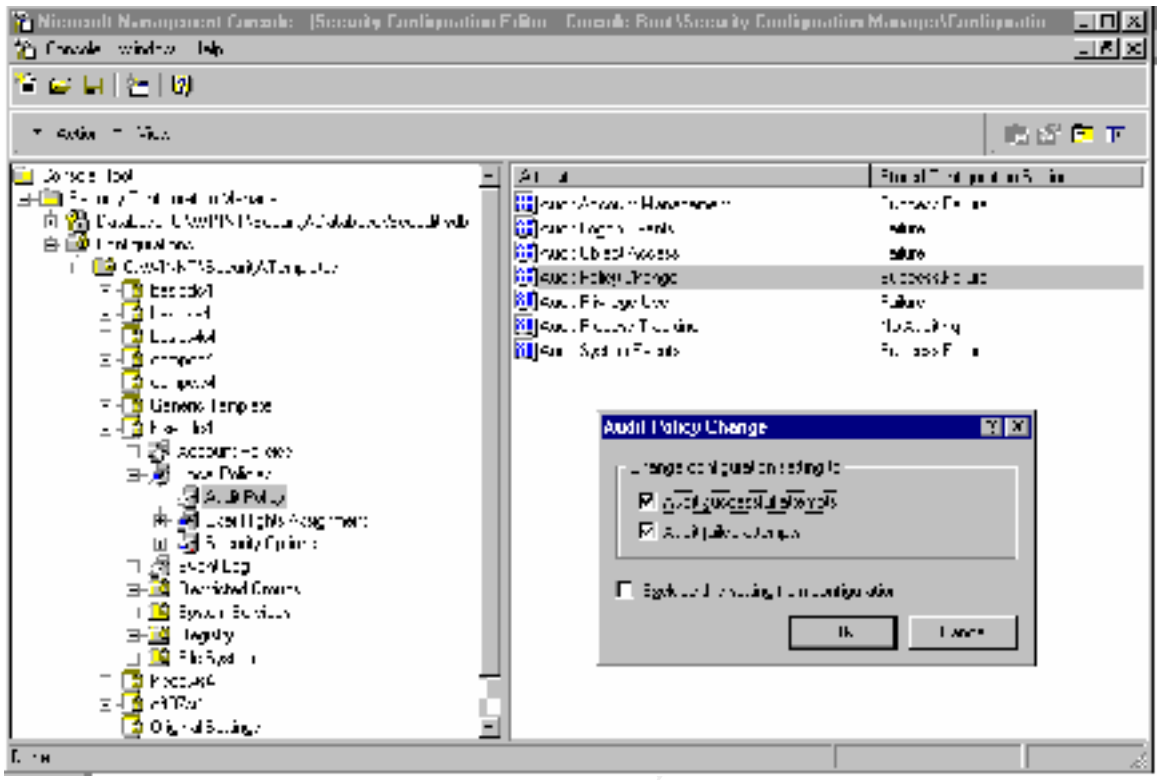

Figure 15: Customizing a Template

After creating customized templates, import the configuration into the database. This activates the template for use in performing a Security Analysis.

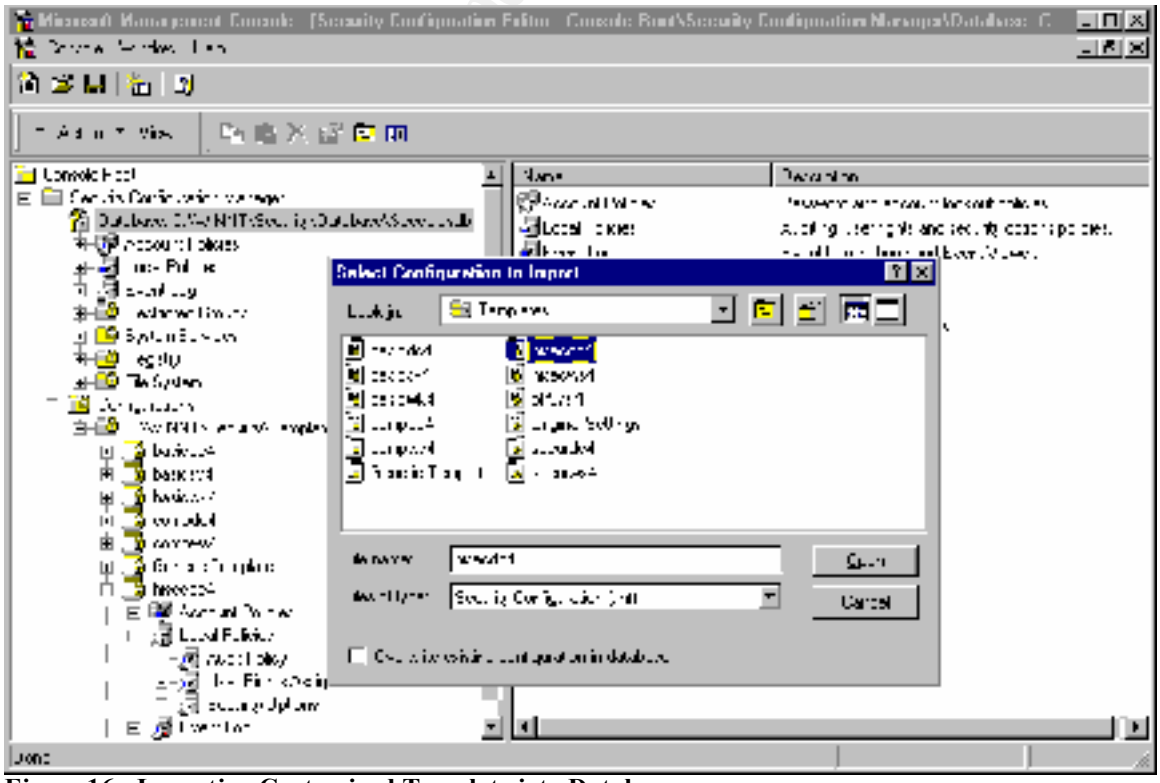

Figure 16: Importing Customized Template into Database

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Performing a Security Analysis

Performing an analysis will compare the local system's security configuration to the customized template in the database.

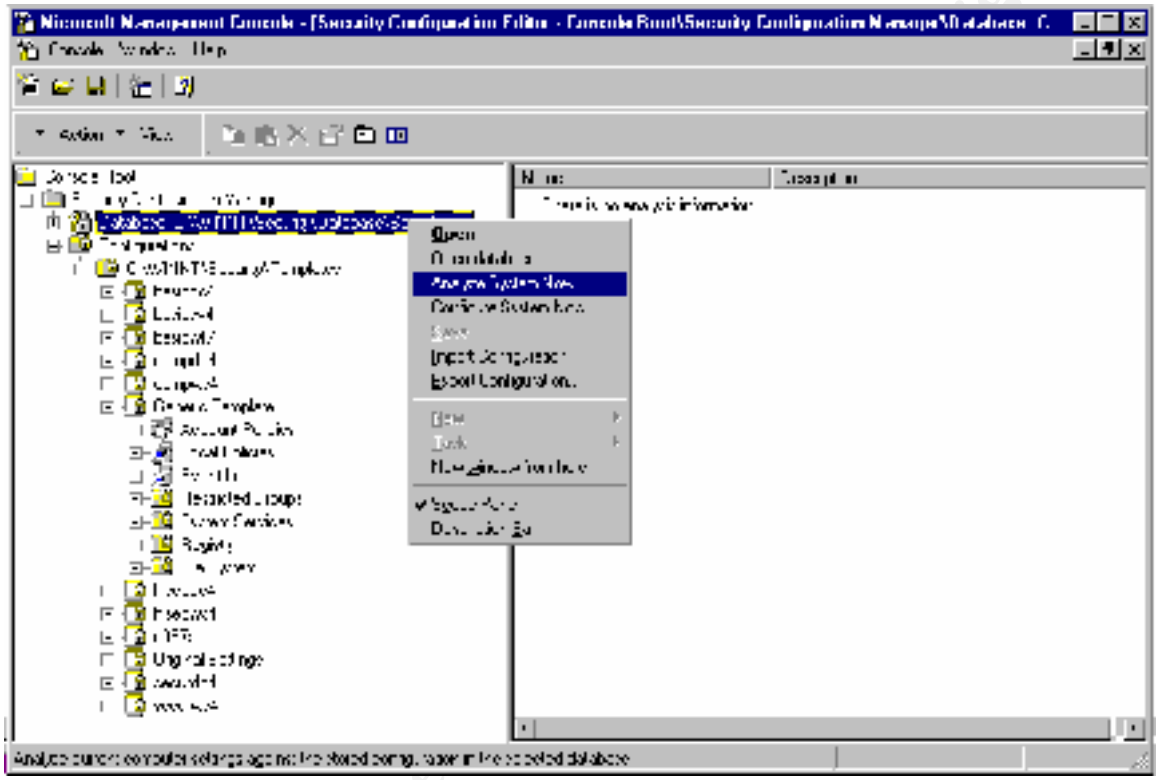

Figure 17: Using the Security Configuration Editor Utility to Perform a Security Analysis

The analysis provides a report that indicates with a red X any deviations from the standard. Note the log size does not comply with the set standard size of 5120 KB.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

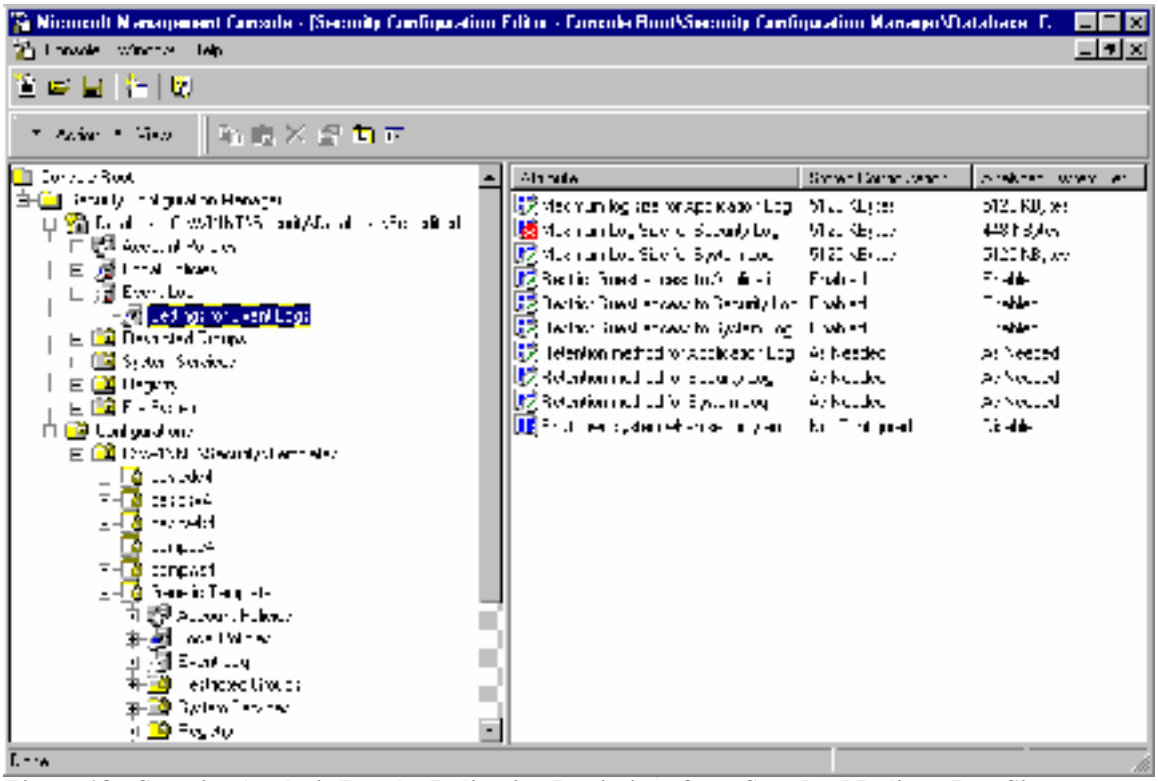

Figure 18: Security Analysis Results Indicating Deviations from Standard Policy– Log Size

Perform analysis on all new systems, after system modifications, and on a regular basis on all systems to ensure compliance.

Bringing a System Into Compliance

After identifying systems not in compliance the *Configure System Now* option will reconfigure the system according to the template imported into the database.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

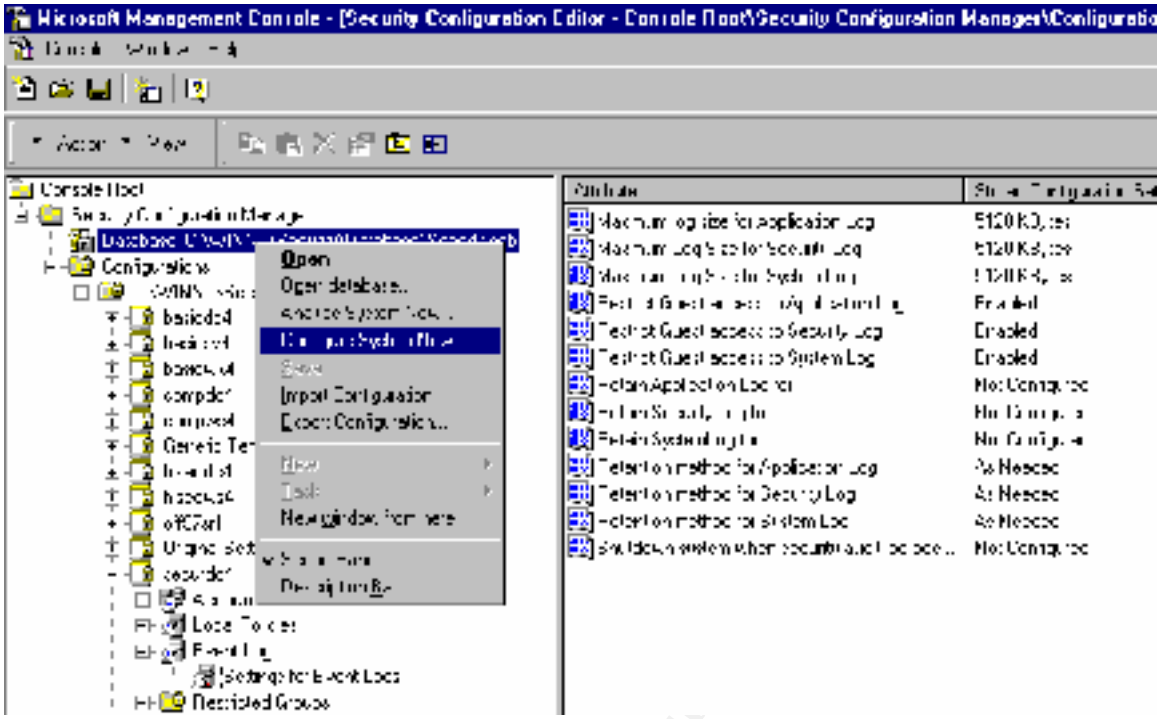

Figure 19: The *Configure System Now* option

The GUI interface configures a local machine. The command line utility, SECEDIT.EXE is available for analyzing and configuring remote hosts.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Command Prompt
C:\>secedit /?

Microsoft(R) Security Configuration Tool Version 1.0 (Windows NT 4.0)
DESCRIPTION: Manage security policies of the system

secedit [/analyze | /configure | /export | /validate]

(1) Configure       Configures your system.
(2) Analyze         Analyze's your systems security settings.
(3) Export        - Generates a configuration template from a database.
(4) Validate      - Validates a configuration template.

Choose a number for more help on the subject: 1

secedit /configure [/cfg filename] [/areas Areas] [/overwrite]
        [/db filename] [/log LogPath] [/verbose] [/quiet]

    /cfg filename       Path to configuration file that will be loaded
                        into the database (/db) prior to performing the
                        configuration.

    /areas Areas        Specifies the security areas to be processed. Default is
                        all areas. Each area should be separated by a space:
       SECURITYPOLICY - Local policy and domain policy for the system.
                        including account policies, audit policies, and etc.
       GROUP_MGMT     - restricted group settings (only for groups
                        specified in profile),
       USER RIGHTS      user logon rights and privilege granting.
       DSOBJECTS      - security on directory objects.
       REGKEYS        - security on local registry keys.
       FILESTORE      - security on local file storage.
       SERVICES         security configuration for all defined services.

    /overwrite        - Specifies that the contents of the database (/db)
                        should be overwritten by the contents of the
                        configuration file (/cfg).

    /db filename      - Path to database that SCE will use to configure the
                        system.
                        If this parameter is not specified, the last
                        configuration/analysis database is used.  If there is
                        no previous database,
                        %windir%\security\database\secedit.sdb is used.

    /log LogPath      - Path to log file for the process. If not provided,
                        progress information is output to the console.

    /verbose          - Specify detailed progress information.
```

Figure 20: SECEDIT.EXE to configure remote hosts

Using NT's scheduler and scripts will greatly enhance the ability to maintain audit and log settings by automating the process of analyzing and reconfiguring systems. Following is a batch file that will analyze and configure a system's security settings in accordance with the template securdc4:

c:\>secedit /analyze /cfg winnt\security\templates\securdc4.inf

Part IV
Common Auditing Practices

Defining an Audit Policy

An organization's Security Policy will include specifications for auditing and logging. The security risks relative to the environment determine what information to log and save. Defining a Security Policy includes identifying service levels, sensitive files, and potential threats.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Auditing should target events that could indicate unauthorized activity, such as repeated unsuccessful logon attempts of the Domain Administrator account. Some environments may decide to periodically log access to sensitive files to verify proper rights assignments. An administrator may want to track the activities of particular users or administrators, or reconstruct a sequence of events to identify and document malicious behavior.

Be cautious not to log so many events that critical events get lost in the sheer volume of data in the logs. Also, be aware that logging full administrators may not provide accurate information as full administrators can change the security log.

Recommended Auditing Practices and Associated Event IDs

Logon and Logoff

Logon and logoff are key events and almost all auditing policies include this selection, as it is a fundamental indication of people's use of the system.

The following logging events will show you who is loging on and off, and the reason for success or failure. Logon attempts from unknown users or from expired accounts could indicate attempted break-ins.

```
   Event ID: 528
      Type: Success Audit
Description: Successful Logon:
            User Name: %1            Domain: %2
            Logon ID: %3             Logon Type: %4
            Logon Process: %5        Authentication Package: %6
            Workstation Name: %7

   Event ID: 529
      Type: Failure Audit
Description: Logon Failure:
            Reason: Unknown user name or bad password
            User Name: %1             Domain: %2
            Logon Type: %3            Logon Process: %4
            Authentication Package: %5 Workstation Name: %6

   Event ID: 530
      Type: Failure Audit
Description: Logon Failure:
            Reason: Account logon time restriction violation
            User Name: %1             Domain: %2
            Logon Type: %3            Logon Process: %4
            Authentication Package: %5 Workstation Name: %6
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
   Event ID: 531
      Type: Failure Audit
Description: Logon Failure:
            Reason: Account currently disabled
            User Name: %1              Domain: %2
            Logon Type: %3             Logon Process: %4
            Authentication Package: %5 Workstation Name: %6

   Event ID: 532
      Type: Failure Audit
Description: Logon Failure:
            Reason: The specified user account has expired
            User Name: %1              Domain: %2
            Logon Type: %3             Logon Process: %4
            Authentication Package: %5 Workstation Name: %6

   Event ID: 533
      Type: Failure Audit
Description: Logon Failure:
            Reason: User not allowed to logon at this computer
            User Name: %1              Domain: %2
            Logon Type: %3             Logon Process: %4
            Authentication Package: %5 Workstation Name: %6

   Event ID: 534
      Type: Failure Audit
Description: Logon Failure:
            Reason: The user has not been granted the requested
logon
            type at this machine
            User Name: %1              Domain: %2
            Logon Type: %3             Logon Process: %4
            Authentication Package: %5 Workstation Name: %6

   Event ID: 535
      Type: Failure Audit
Description: Logon Failure:
            Reason: The specified account's password has expired
            User Name: %1              Domain: %2
            Logon Type: %3             Logon Process: %4
            Authentication Package: %5 Workstation Name: %6

   Event ID: 538
      Type: Success Audit
Description: User Logoff:
            User Name: %1             Domain: %2
            Logon ID: %3              Logon Type: %4

   Event ID: 539
      Type: Failure Audit
Description: Logon Failure:
            Reason: Account locked out
            User Name: %1              Domain: %2
            Logon Type: %3             Logon Process: %4
            Authentication Package: %5 Workstation Name: %6
```

Interpreting the events includes an understanding of the different types of logons.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The logon type indicates how a user successfully logged on. Event ID 528, Type 2 indicates a console logon. Event ID 528, Type 3 indicates a connection over the network, such a through a drive mapping. A Type 5 login indicates a service logon and Type 4 is a batch job logon. You will see a Type 7 logon when a user unlocks a workstation.

Event ID 538 is ID 528's corresponding logoff event. This provides the duration of the user's logon session. This information provides a history of a user's successful access to a particular computer.

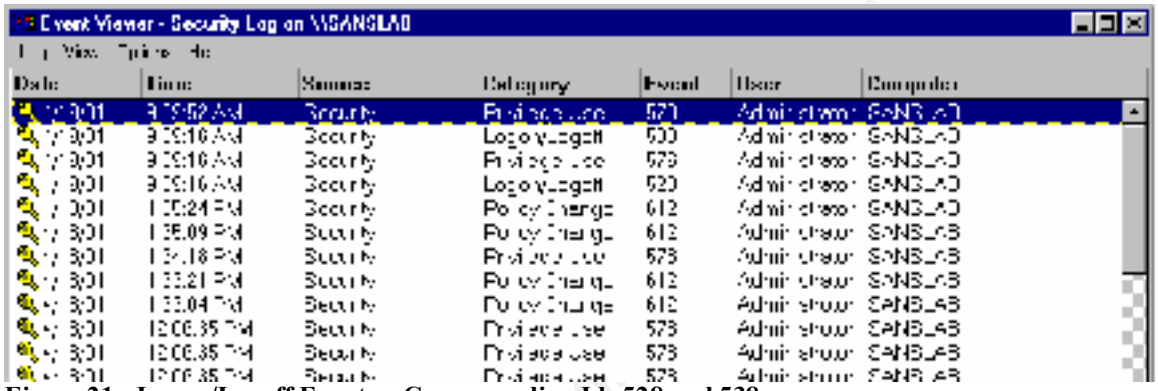

Figure 21: Logon/Logoff Events – Corresponding Ids 528 and 538

Figure 22: Logon Type 7 – Unlocking a Workstation

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The most common logon failure, Event ID 529, results in the message *Unkown user name or bad password*. Multiple Event IDs 529 may alert an administrator to a possible brute force attack.

Startup, Shutdown, and System

All policies should include auditing this activity. Many times servers are located in out-of-the-way rooms, providing ideal cover for an intruder. An unexpected startup or shutdown event may indicate an improperly secured machine, an intrusion, or a system crash. Utilities exist that allow remote reboots, a different type of security threat that might indicate an intruder's attempt to activate a Trojan.

The Event IDs associated with startup and shutdown are:

```
   Event ID: 512
       Type: Success Audit
Description: Windows NT is starting up.

   Event ID: 513
       Type: Success Audit
Description: Windows NT is shutting down. All logon sessions will
be terminated by this shutdown.
```

Security Policy Changes – all policies should audit changes to the security policy as it effects what events are actually written to the log files. An administrator relies on log files and must be confident that they are reflecting intended information. Changes to Audit and Rights policies are infrequent occurrences and unauthorized changes may indicate an intruder's or malicious administrator's attempts to cover tracks.

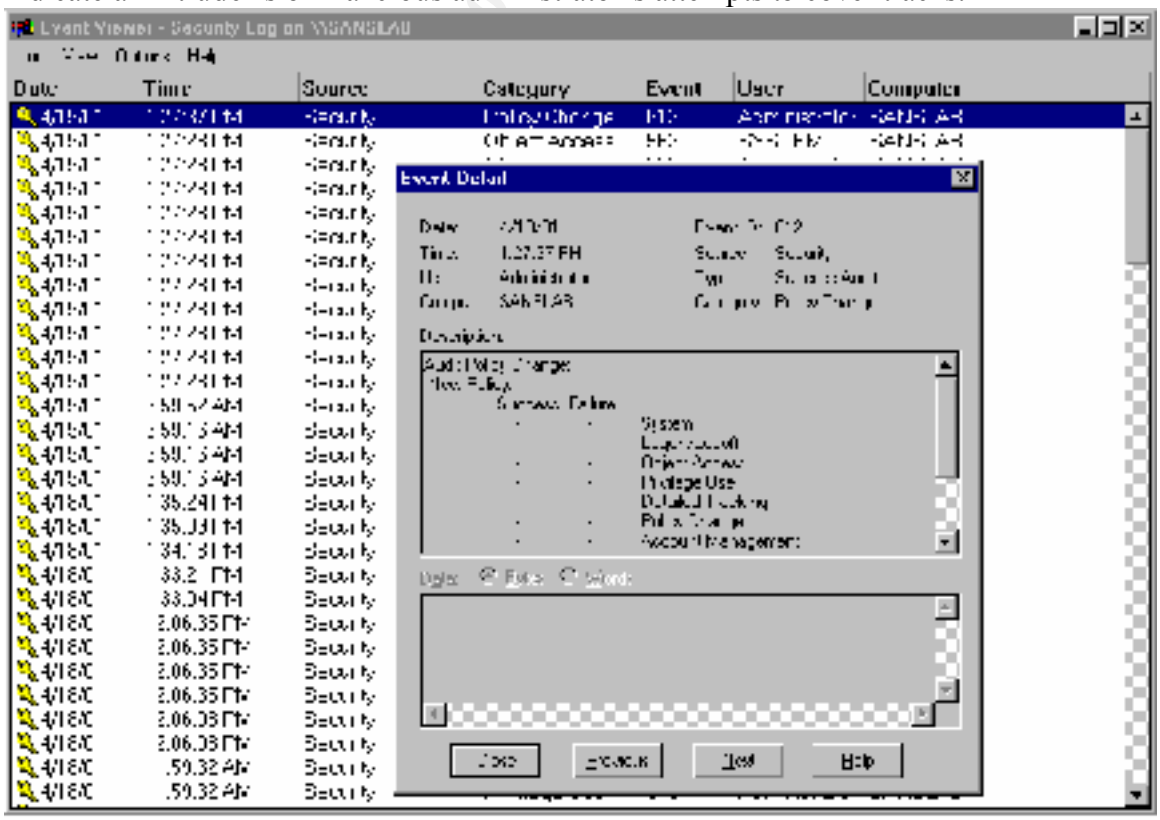

Figure 23: Event Detail Policy Change – turning off all logging

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Also, it is critical to monitor the event ids associated with the log files.

```
   Event ID: 516
       Type: Success Audit
Description: Internal resources allocated for the queuing of audit
             messages have been exhausted, leading to the loss of
some audits.
             Number of audit messages discarded: %1

   Event ID: 517
      Type: Success Audit
Description: The audit log was cleared
             Primary User Name: %1      Primary Domain: %2
             Primary Logon ID: %3       Client User Name: %4
             Client Domain: %5          Client Logon ID: %6
```

User and Group Management

These events provide a log of administrator's activities. An intruder will attempt to obtain administrator level privileges as it allows further compromising the system. A security administrator may also want to audit these events to ensure that multiple administrators are coordinating their activities and in the process are not creating any security holes.

Events to monitor include checking for additions to the Administrators group, creation of new accounts and to which groups they were added.

Event IDs associated with changes to the Administrator's group:

```
   Event ID: 632
      Type: Success Audit
Description: Global Group Member Added:
             Member: %1                 Target Account Name: %2
             Target Domain: %3          Target Account ID: %4
             Caller User Name: %5       Caller Domain: %6
             Caller Logon ID: %7        Privileges: %8

   Event ID: 633
      Type: Success Audit
Description: Global Group Member Removed:
             Member: %1                 Target Account Name: %2
             Target Domain: %3          Target Account ID: %4
             Caller User Name: %5       Caller Domain: %6
             Caller Logon ID: %7        Privileges: %8
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

New user accounts:

```
     Event ID: 624
        Type: Success Audit
  Description: User Account Created:
               New Account Name: %1        New Domain: %2
               New Account ID: %3          Caller User Name: %4
               Caller Domain: %5           Caller Logon ID: %6
               Privileges %7
```

File and Object Access

Logging file access can generate voluminous data and has the potential of slowing down system performance depending on how many object you audit and how often they are accessed. Auditing highly important resources is critical, however, object access should be used sparingly. Critical files to audit include an organization's sensitive material such as financial information, human resources, business strategy, etc. This auditing information ensures proper access permissions. Other files a security administrator might want to audit include access or changes to the SAM, the registry, or other operating system files that might indicate an intrusion.

The object access category has three events: 1) Event ID 560, *object opened*, 2) Event ID 562, *handle closed*, and 3) Event ID 564 *object deleted*. The two main events, Ids 560 and 562 are complementary events similar to the logon and logoff events, and allow an administrator to determine the length of time the user had the object open. Objects can be accessed different ways, the same way logon and logoff events indicate different types of logons.

The event detail will show the logon session of the user and will indicate if the user accessed the object directly or through a client/server application. For example, if a user accesses a file share over the network, the user's local workstation service connects to the server service on the remote system. In this case, the Primary User Name is System and the Client User Name is the user's logon id. Accessing a file on a local system will indicate the user's logon id as the Primary User Name.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

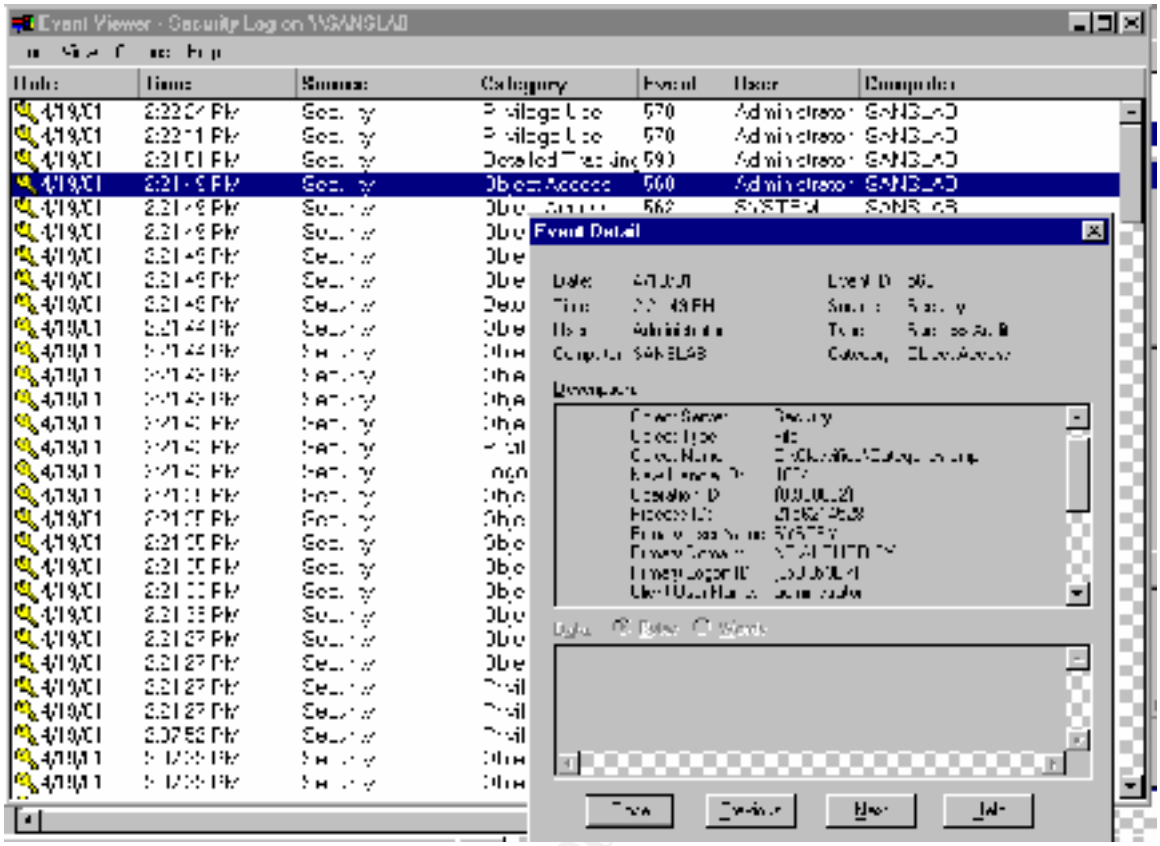

Figure 24: Event ID 560 – Object Access, System as Primary User

The object access category *object deleted*, Event ID 564, indicates a Handle ID and Process ID. Linking the Handle ID, Event ID 564, to the corresponding object opened event, Event ID 560, identifies the user and the object deleted.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

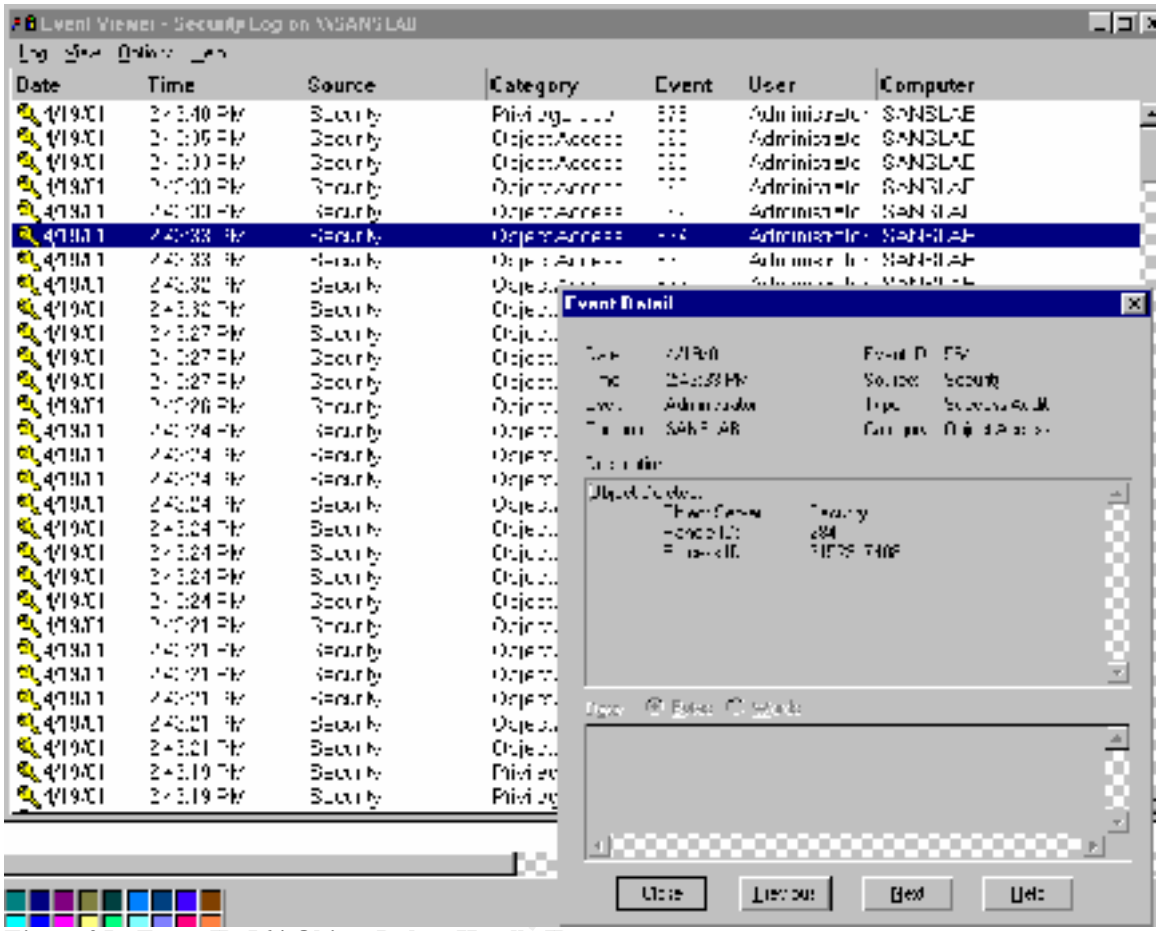

Figure 25: Event ID 564 Object Delete Handle ID

© SANS Institute 2000

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

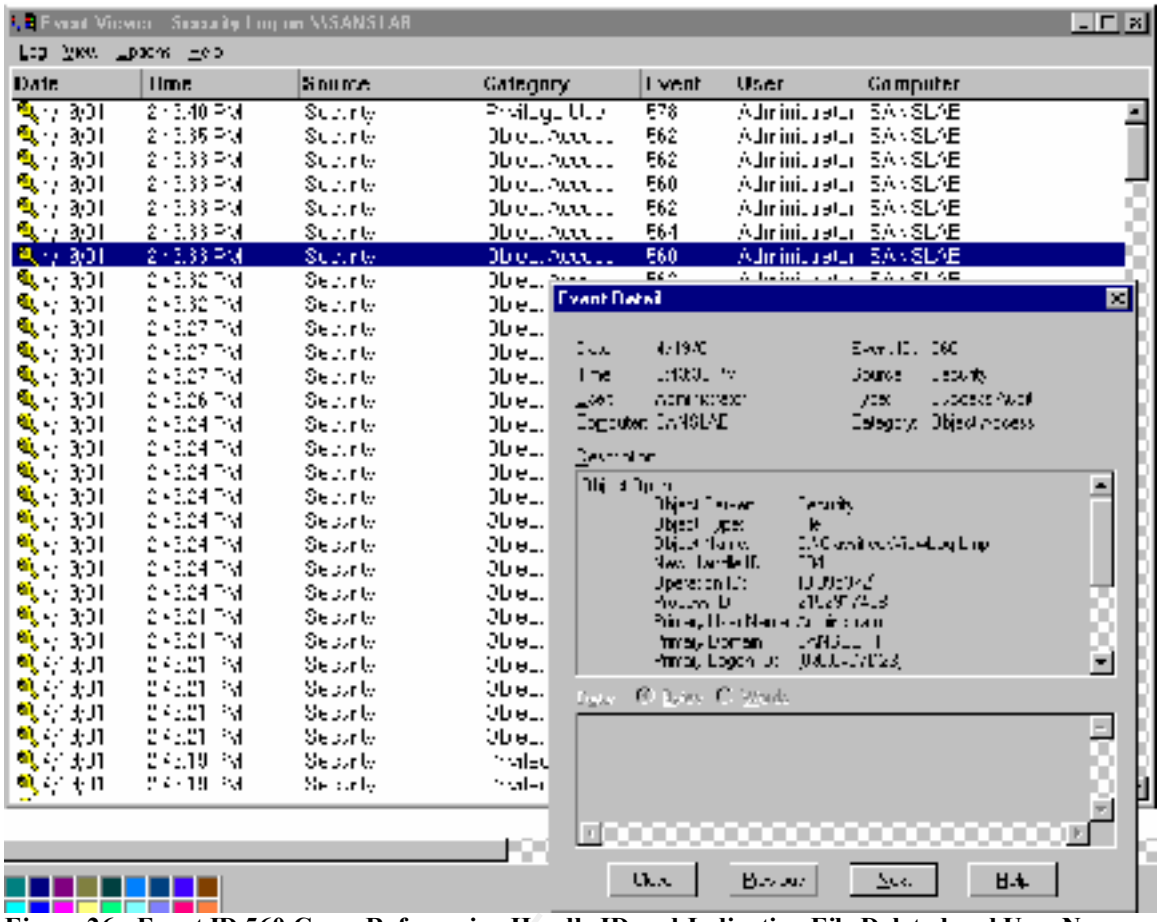

Figure 26: Event ID 560 Cross-Referencing Handle ID and Indicating File Deleted and User Name

As a reminder and as mentioned above in Part I Step 2, enabling object access auditing is a two-step process. First object auditing must be enabled in User Manager by selecting the category, and then specific directories and files are selected for auditing.

Process Tracking

Process tracking tracks which programs a user is running on a workstation and which programs a server is running. Auditing these events, when combined with object access auditing, are useful when it is necessary to investigate a user's activities. The Event Details indicate which executable a user opened, by which user, and when the process was exited.

The two events associated with process tracking are Event ID 592, *creating a new process*, and Event ID 593, *exiting a process*.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

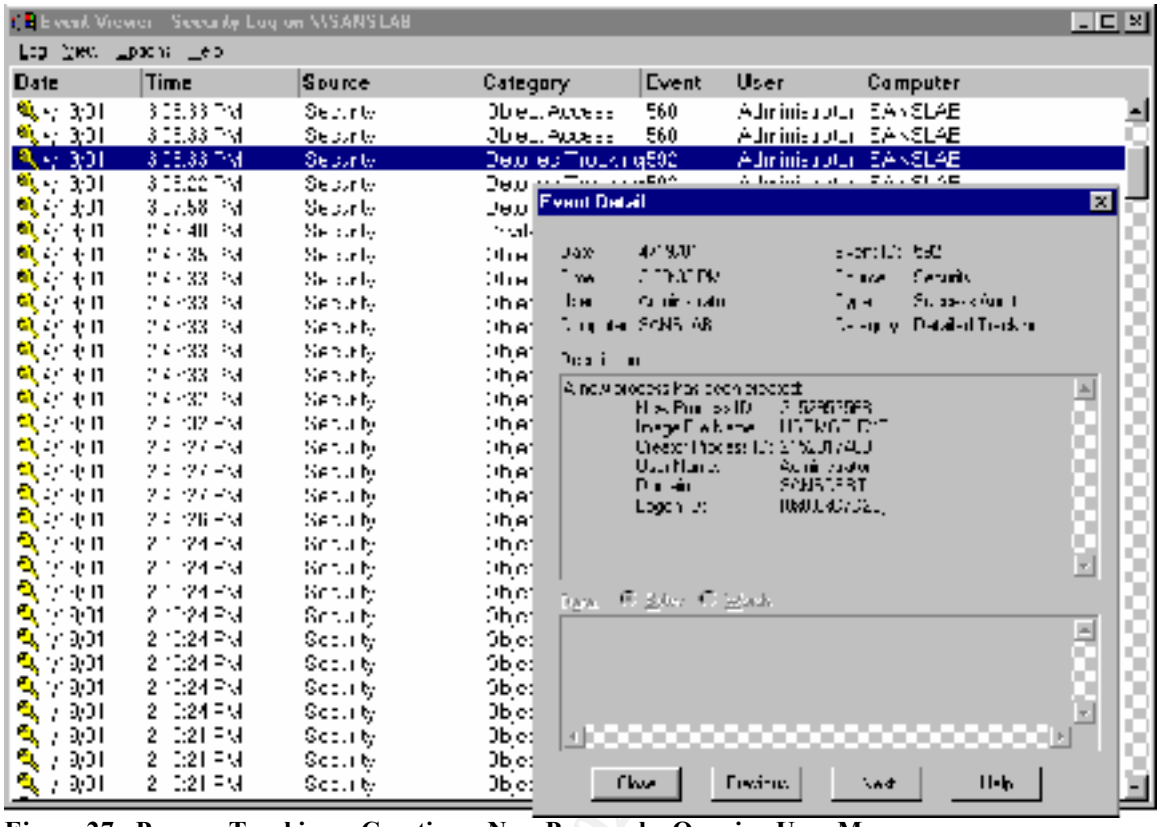

Figure 27: Process Tracking – Creating a New Process by Opening User Manager

Conclusion

Utilizing NT's Auditing feature provides an additional layer of security allowing security administrators to track unauthorized activity. While auditing is a record of what has already happened, it can be useful in preventing further intrusion, and for exposing weaknesses in your existing security system. Auditing provides a history of changes made to the system, and it can provide the information necessary to prosecute an attacker, or identify malicious administrators.

Key to utilizing auditing effectively is managing the log files. Regular review of log files, sorting for key information, proper log file configuration and archive procedures requires planning and coordination with the organization's security policy.

Because networks and systems are almost always in a state of change it is critical to maintain the standards set for auditing practices. Microsoft's Security Configuration Manager provides an excellent method for reviewing and identifying non-compliant systems. It also provides centralized management features that make it simple to bring non-compliant systems into compliance as soon as they are identified. It can also be used to ensure new systems added to the network are within compliance.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

NT's scheduler and batch files greatly enhance the ability to maximize the benefits of auditing by automating procedures. Use the DUMPEL utility to preserve log file data; use the SECEDIT utility to ensure system compliance; create files highlighting significant security events using the DUMPEL utility to sort event ids; and use the AT command to automate and schedule these tasks on a regular basis. Intrusion Detection Systems provide similar services as these utilities, as well as provide the added benefits of user-friendly interfaces and reports, and automated alerts.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

Brenton, Chris, Mastering Network Security. Alameda, California: SYBEX Inc., 1999. 70-71.

Anonymous, Maximum Security, A Hacker's Guide to Protecting your Internet Site and Network, Second Edition. Indianapolis, Indiana: Sams Publishing, 1998. 70-71.

Sutton, Stephen A., Windows NT Security Guide. Reading, Massachusetts: Trusted Systems Services, Inc., 1997. 193-221.

Smith, R. Franklin. "The NT Security Log – Your Best and Last Defense." 3 August 2000. URL: http://www.microsoft.TechNet/winnt/ntsecuri.asp (28 March 2001).

Smith, R. Franklin. "Interpreting the NT Security Log – Use the Security Log to track user's activities." 4 August 2000. URL: http://www.microsoft.TechNet/winnt/ntsecuri.asp (28 March 2001).

"MS Security Configuration Manager for Windows NT 4 White Paper." 12 January 2000. URL: http://www.microsoft.com/technet.winnt/winntas/technote/scmnt4.asp (23 March 2001).

"Security Event Descriptions." 21 June 2000. URL: http://support.microsoft.com/support/kb/articles/q174/0/74.asp (23 March 2001).

"Automating Detection of Logon Failures in a Windows NT Domain." Microsoft article PSS IS Number Q171148. 21 March 2000.

"DUMPEL.EXE Can Interpret Log Hex Data." Microsoft article PSS IS Number Q129266. 26 February 1999.

"Automating Detection of Logon Failures In a Windows NT Domain." Microsoft article PSS IS Number Q171148. 21 February 2000.

Heckendorn, Sherri. "Sherri_Heckendorn.doc." URL: http://www.sans.org/y2k/practical/Sherri_Heckendorn.doc (23 March 2001).

Yeo, Lisa. "Configuring and Auditing Windows NT with Security Configuration Manager." September 2000. URL: http://www.sans.org/giactc/gcnt.htm (23 March 2001).

Toy, Steven. "Centralized Auditing of a Windows NT Computer." URL: http://www.sans.org/giactc/gcnt.htm (23 March 2001).

Gabert, Howard F. "Using Event Logs to Audit Windows NT4." August 2000. URL: http://www.sans.org/giactc/gcnt.htm (23 March 2001).

Carboni, Christopher. "Christopher_Carboni.doc." URL: http://www.sans.org/giactc/gcnt.htm (23 March 2001).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Jain, Anil K. "Developments in Auditing NT." URL: http://www.sans.org/giactc/gcnt.htm (23 March 2001).

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: April 28th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Security West 2017	**San Diego, CA**	**May 09, 2017 - May 18, 2017**	**Live Event**
SANS Northern Virginia - Reston 2017	**Reston, VA**	**May 21, 2017 - May 26, 2017**	**Live Event**
SANS Cyber Defence Canberra 2017	**Canberra, Australia**	**Jun 26, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
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**
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 OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**