

# **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.

# WINDOWS NT AUDITING SECURING YOUR NETWORK

SANS GCNT PRACTICAL ASSIGNMENT MAY 2001 KATHRYN SALYERS

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

# TABLE OF FIGURES

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

Page

# 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

### Event Categories

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.

Audit Policy			×
firman SANSEL II			OK
O Do No: Audi			Cancel
- 🕤 Audit Theos Events:			1
	Success	Faiure	Нөр
Logon and Logof	M	Μ	
File and Object Access	M	Μ	
Los of User Richto	Г	Ē	
Uver end <u>G</u> idoù Mariagenen.	9	M	
Security Policy Changes	M	4	
$\underline{L}$ estail, Shultdown, and System	М	М	
Emcess Liefking			

Figure 1: Event Categories

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

In User Manager ... Logon and Logoff File and Object Access Use of User Rights User and Group Management Security Policy Changes Process Tracking Restart, Shutdown, and System

In Event Viewer ... Logon/Logoff Object Access Privilege Use Account Management Policy Change Detailed Tracking 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.

#### Event Viewer

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.

Ling Meets	Dations Holp					
Date	Linus	Summe:	Enlogency	Even	Uncer	Docquetes
🔪 <i>(9</i> 0	1 50:00 PM	Ges. w	Policy Crance	2.2	Administrator	SAN3LAD
60 6, 160	2 53,35 FM	Selling	Policy Tranco	2.2	Administrator	SANSLAS
Q.430	2 50.43 FM	Sell' M	Policy Pronze	3.2	Administrour	SANGLAB
Qiệ (chi t	12/28/41110	Sec. 2 yr	Dany Chinese	-75	A lu cistu re	SANH AR
Çéér –	17/28/241162	Setury	Linuxy Cronge		Administroor	SAN-CAR
Castr	17.27° × HM	ter, ý	Houry Change	·*>	Administration	SANK A L
€ 190° -	10.27:00 FM	Ges. 🗙	Policy Crange	212	Administrator	SANGLAD
S. (40 -	0.27:00 PM	Ges. ŵ	Policy Drande	3.2	Administrator	SANGLAD
🔍 - 30	2 26.35 PM	Sellin	Policy Pronce	3.2	Administrour	SANGLAB
(	206 205/	SH	Duity & more	3.2	Abirstoor	
gure 2:	Event Viewer	/View/Log				

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.

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

### The User Manager utility

rame Fr	d I Nume		Description
Audit Policy			I country atmosteling the conculary commu-
Donew CANTOTOT C. Dir Son And —⊗ Şauli Thurse E-ser Ja			OK Graz Graz GyDept
Luger Line LugerY Lip and Ubject Access Qire of User Hights History I South Olano parter Security Folias Chances Russelly Shatdoong Line South Princips Tundung	य य य य य	न व व व व व र	

Figure 3: The User Manager Utility/Audit Policy Events

The Microsoft Management Console utility



Figure 4: Microsoft Management Console/Security Configuration Editor

A trainer for the Second View of the Second V	₩ Manana II Na scoper of Consular - (Secondar Configuration 10 genetik - 2010 - 2010) 2011 - 2011 - 2010	i Fal tao - Caonada Roat/Konsoly Confi	presión e les esta nel Carelliperatione (C. 1971)	HHTUSinnai yi Tingi Laine Lanani
Care L Res     All the set of	ŭ≉∎inin Internet			50
Presidential and a second distribution of the second distr	Ans.4. Parkey Change:     [2] [2]       One open objective sector to the participanetic sector to the participane	<ul> <li>Astrophysic Version Life</li> <li>Astrophysic Version</li> </ul>	Successification Datas Notice 19 Notice 19 Datas Datas Notice 19	

Figure 5: Audit Policy Changes in Security Configuration Editor

<u>Step 2</u> – 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

### The Security Configuration Manager utility



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.

### Event Viewer

DK -	1
Cancel	1
Defaut	
Help	Ś
	Carcel Defeut

Figure 8: Using Event Viewer to Configure Log Settings

Microsoft Management Console

The Niciosoff Newsgement Contate - (Security Configure	abon Editor - Cansale Haal/Geouniy Configuration	Manaper@configuratio
The Sanah Wards Hale		×
월 6월 1월		
<ul> <li>Cancer Book</li> <li>Such (Configuration Hanager)</li> <li>Configuration Hanager)</li> <li>Configuration:</li> <li>Co</li></ul>		Source Complexact Setting 2980 KBrow 2987 A Frank 2987 A Frank 2088 A Brow 2088 A Brow 208
F •• A		

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

# 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.

### **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.

Джи Прэсия Пер					
ten:	Source	Category	Event	Uden	Computer
ery 💼	Security	Fullipy Chonce	3.2	Administration	SANSLAE
Lodech	Security	Pelicy Chonce	3.2	Administro.or	SANSLAE
-	Security	Pelicy Chonce	3.2	Administro.or	SANSLAE
n.	Security	Pelicy Chonce	32	Administro.or	SANSLAE
e Awi	Second	Fchuly Chonce	52	Administration	SANSLAE
n/Hurwits	Second 1	h h y Chunne	57	Administration	SANSI AF
- i p	Second 1	They Crimine	52	Administration	SANSI AF
.,	Second 1	They Crimine	52	Administration	SANSI AF
of Computer	Servey	Foliny Cronce	52	- Administrement	SANSI AF
All all A	Servey	Foliny Cronce	57	-administrement	SANSI AF
·	Servey	ictity Cronge	52	-administreme	SANSI AF
QU1 1217/30 PM	Secury	ichty Cronge	52	Administreet	SANSI AF
Q11 121140 PM	) enury	Clin Cronce	52	Administration	SANSI AH

Event Viewer provides an option to save log files.

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.

		_
🔀 Command Prompt		
D:\Tools\evtools>dur	npel ?	
DUMPEL Usage:		
dumpel −f file [−s ヽ x]	<pre>\\server] [-1 log [-m source]] [-e n1 n2 n3] [-r] [-t] [-</pre>	-d
-d <days) -e nn -f <filename) -l <name) -b -m <name) -r -s <servername) -t -c -ns -format <fmt)< td=""><td><pre>Filters for event last days (number larger than zero) Filters for event id nn (up to 10 may be specified) Output filename (default stdout) Dumps the specified log (system, application, security) Dumps a backup file (use -1 to specify file name) Filters for events logged by name Filters out events logged by name (must use -m too) Remote to servername Use tab to separate strings (default is space) Use comma to separate fields Do not output format. Default format is dtTClSucs where t - time d - date T - event type C - event source u - user c - computer s - strings</pre></td><td></td></fmt)<></servername) </name) </name) </filename) </days) 	<pre>Filters for event last days (number larger than zero) Filters for event id nn (up to 10 may be specified) Output filename (default stdout) Dumps the specified log (system, application, security) Dumps a backup file (use -1 to specify file name) Filters for events logged by name Filters out events logged by name (must use -m too) Remote to servername Use tab to separate strings (default is space) Use comma to separate fields Do not output format. Default format is dtTClSucs where t - time d - date T - event type C - event source u - user c - computer s - strings</pre>	

Figure 11: DUMPEL.EXE

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

🔀 Command Prompt	
	e] [ [id] [/DELETE]   /DELETE [/YES]]
	e] 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
(auguutdata [ ]	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[,]	
	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

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.

Mew From       View Through       1 K         Image: Events Qr:       Image: Events Qr       Image: Events Qr         Image: Im
E <u>v</u> ert C.

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

Logon Type: %3

Authentication Package: %5 Workstation Name: %6
```

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* (<u>http://www.iss.net</u>). 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.



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.

🚡 Micansoft Management Consule - [Sa	assity Configuration P	Fuitor - Console Bout\Sc	and y Condig	nation Narsopa/Database 🖒 📲	. П X
🏫 Sevena Section Lan				-	
19 3 M 12 19					
] T Adia T Viss   陸山區 米 🗟	° 🖻 M				
🔄 Console Ficel	1	Nane	Dev	ani no	
E 🗎 Certris Conintration vaneger		💬 Accessi Marine	1400	earth and encount indications.	
🐴 Duclares I.V./ NHT/Sec. ig/0.	(derectional)	Eccal order	A. 16	ing user rights and security opports polic	#:.
年(愛 ∧ccourd blass		delikeren tur		d have have any keep to see a	
at-add no-Polles जिल्ली s-add aug	Select Configuration	in Import			
🕸 🔛 – externer limerz	Lukju 🔄 Ten	p	J 🖬 🖆		
ij <mark>199</mark> š∧turšuvuva Li ov	📓 de A	a water of		`	
₩ <u>₩</u> es#0		NAMES N			
— — — — — — — — — — — — — — — — —		is atan ≸atan			
<ul> <li>Identification</li> <li>Identification</li> <li>Identification</li> </ul>		անակում։ 📓 Հայաստ Երկերը			
		🖌 allender			
回, a bativetee 图 ···································	Janeie Tag 1	al - as,o∸			
🖌 🏹 hadaari	<b>D</b>				
Fi 🛃 contadol					
🗄 🏹 contrewi					
ជ្រ 🏹 ចំពោះ ហើយត្រោះ	de namer - weevin	1		Sec. 1	
🖞 🍮 three 524	Avertigen Securiz	Configuration (Initia	-	Carcel	
E 🖼 Averani Do rev				Carte	
」 (遺 Lust Fakitz					
- <u>@</u> (Accipity)	Country of the Country of Country	uni garat on in databuro			
≞->⊒ lie Fit c>ciu		1			
i ≣ ja suura yi Jalaan ≣ ≣ ina suura yi					
E 🖉 Eventor	<u> </u>	<u> </u>			
Jone					li.

Figure 16: Importing Customized Template into Database

# 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.

🚡 Nicocolt Nanagement Canade - (Seconity Canfiguration	Filter - Fancole BootStecority Camb	quation Manage/Ma	
📸 Linovole – Winchos – Leip			_ <b>- -</b> X
- Azim + Hex - Ali 南 × 雪 南 市			
🛄 Conversion Root 🔹 🖉	Alabade	Some Danas seas	whether when an
由 🛄 Genety I nit geni no Hervijes	🐯 visorium log see vor spolikisto r Logi	51., 31.09	512. KD, **
📮 🖓 fajal 🗵 Chwhiththis anitAfalai - Nichailte 🗌	📕 Mashan Lo, Sue e Sabady Lo		491326
「 関 Award Arass	😥 Makran Lou Silv 'a Systematic	•	5120 NB, 444
E 🖉 Land Thease	📝 Bertin: Smed - ress tu A 🖷 - i		
L ) 🗃 Evertua	📝 Dectric: Duest encourts Depurity Lon-		Trables
L — _@ <mark>i Leding: wituestilling:</mark> I — E. <mark>∭2</mark> Devertied Tarapa	😥 letter field show to fyden ing	Lineb ett.	-shier
E Sector Service	😥 Idenion netted wiscoketer Leg	At Nesdec	ia: Neeced
	🔣 Relation real and on subary log 🌷	Av Nordeo	Ar Needed
L E C F - PO F (	😥 Setation net et la Systemator	Av Nordeo	Ar Noticed
🗆 🗃 Calgaston:	🕕 Erst versyder of er de lit yer	to The post	Té dé-
E 🙀 Do-TAN Security Lemmes	II .		
_ 👔s.aket			
7-🚺 25:23-4			
<mark>_3</mark> ••/ ••lot			
🔯 (g 4			
E-📑 conpost			
in the second se	9		
市 郡 Autour, Huleau 東山湖 Toos (Mines	9		
#- <b>2</b> 1 - 2019 - 2019	8		
n jarstviste n jarstviste	01		
H Diview Process	9		
T - ·	al		
Long Land			
1 <b>n</b>			

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.



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.

🔀 Command Prompt		_ 2 ×
	Configuration Tool Version 1.0 (Windows NF 4.0) ecurity policies of the system	-
acceptit (Annalysic ( $\Delta$	configure : Zesport : Zvalidate)	
(2) Analyse Analyse Analyse Control (3) Analyse Ana	nfigures your system. alyze's your systems security settings. nerates a configuration template from a database. Ifdates a configuration template.	
Choose a number for a	are help on the subject: 1	
cecedit /configure LA E/dh filename	cFg filenamel L/areas Areas]  /overwrite]   [/log LogPath] [/verhose] [/quiet]	
∕cfg lilename	Path to configuration file that will be loaded into the database (Adb) prior to performing the configuration.	
CROUP_MONT USER REGNES DSOBJECTS RECKEYS PELESTORE SEDUICES	<ul> <li>Specifies the security areas to be processed. Default all areas. Each area should be separated by a space:</li> <li>Local pulicy and donain pulicy for the system. including account pulicies, audit pulicies, and etc.</li> <li>restricted group settings (only for groups specified in profile), user logon rights and privilage granting.</li> <li>security on directory objects.</li> <li>security on local file storage, security configuration for all defined services.</li> </ul>	
/overwrite -	Specifies that the contents of the database C/db) should be overwritten by the contents of the configuration file $\langle /cf_T \rangle$ .	
Alb 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 provious database. XwindirX'vecuritg'vlatabase\secodit.cdb is used.	
∕log LogPath -	Path to lag file for the process. If not provided, progress information is autput to the cansole.	
Zvenboce -	Specify detailed progress information.	
Figure 20. SECEDIT FX	E to configure remote hosts	

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. 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
```

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: Domain: %2 Logon Type: %4 User Name: %1 Logon ID: %3 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.

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.

Li ji Mixe T	war-Security Lag juine Ho						
Dalo	Linu:	Summer	Delogory	Event	Hoor	Durquider	
<b>4</b> 12 901	8 19:52 AM	Becarby	Environauco	570	Administratory	SAN3 AT	
<b>0,</b> 7/ 9/01	9 09:10 AM	Becurity	Logo yuqqafi	500	Administrator	SANGLAD	
S, 7 9,01	9 09:10 AM	Becurity	Fridade Loo	579	Administrator	SANGLAD	
S, 7 9,01	B 05:16 AM	Becurity	Logo yuqqati	520	Administrator	SANGLAD	
🔍 / QOL -	100:24 FM	Beetrie	Policy Intergo	612	Administrator	SANGLAD	
📢 sjor -	1 35.09 Ptd	Stark	For the Indian	612	Admin Chator	SANSLAB	
🔍 () S(OL –	1.34,18 PM	Stark	Proibeo de	573	Admin Chator	SANSLAB	
🕵 () S(OL –	1 33.21 PM	Scorte	Policy their gu	612	Admin Chator	SANSLAB	
🔍 ને સંગા	1 33.04 PM	Security.	Policy that get	612	Administroup	SANGLAB	
🔍 - 2 3 O I 👘	12 C6.35 PM	Decci N	Drviece use	573	Administro.or	SANGLAB	
N 301	12 06:35 7:4	Decurity	Projece Jae	573	Administroup		
🔍 ને સંગો	12 CE 35 PM	Second-	Drvi apa Use	573	Administration	SANG AB	

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

Event De	tail			×
imer Llaer	47 E/01 9+9106 AM Administrator en SANSTAN	50°°	Security.	
Descript	ion:			
місар	sful Locor: Use: Name: Domain Logon ID. Logon Type: Logon Process 4. theolitiannel ! SCFT_AUTHENTIC Works: at on Nam	FORADE DATION_PACKAGE_ ne: SANELAE	V1_0	T I
				4
	Clove Blav	ruly <u>N</u> ext	<u></u> =	

Figure 22: Logon Type 7 – Unlocking a Workstation

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 outof-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.

📫 Liyant Yis	NINE - Security Log	on MSANSE	4U	
10 Yes (	Ottore H-Aj			
Date	Time	Source	Category Event User Computer	
a, 4090 n	1223/144	-iecurity	Unloy Charge 140 April restrict Ref. 48	
<b>%</b> 47537	12224144	-i=curity	Of emergences (FF)77 FM6-M-6 A-8	
<b>3</b> 4793 *	1022281.44	-terautity	Every Delaid	
<b>%</b> 47537	1022281.44	-terautity	Every Delali	
<b>%</b> 47937	12228144	-terautity	Delet 7/10/01 Event 3: 012	
<b>%</b> 4753 *	1022281.44	-terautity		
<b>%</b> 47937	1002281.04	-terautity	Tine 1.27.37 FH Scale Scale,	
<b>%</b> 4/19/17	107728144	-l-rainly	He Administration Two Status e Annal Communications Communications	
N 4754 T	107728144	-l-rainly	Comp. SANELAS Compro Prior Transp	
N 479-7	107728144	-l-rainly	Description	
N 4797	10728144	-l-rainly	Aud of Veloy Changes	
<b>%</b> 4/19/17	12778144	-l-rainly	they Fulk a	
N 4754 T	+59 52 AM	-l-rainly	Simples Extension	
<b>%</b> 47501	5 59,1 3 AM	deanly.	<ul> <li>System Lager Accord</li> </ul>	24
<b>%</b> 4/15/01	259/13404	deanly.	Conjection of the second	24
<b>%</b> 4/15/UT	2 59/13 444	deanly.	Thickege Use	24
<b>3</b> 4780°	1 35.241 14	deanly.	Dutaku Fucking	24
<b>4</b> 4180°	1 35.J31 f4	deanly.	<ul> <li>Politik Transport</li> <li>Account Mainagement</li> </ul>	24
<b>%</b> 4780°	1 34,131 14	deanly.		24
N3174 SC	33.2 Ft-1	Beauty	Digles C Ester C Science	- 21
N314/	33.34 Ft-1	Beauty.		- 21
N314.	2.06.35 Ft-1	Beauty.		- 29
<b>%</b> 4/18/C	2.06.35 Ft-1	Beauty.		- 24
N3174	2.06.35 Ft-1	Beauty.	21	- 24
<b>3</b> 4/18/C	2.06.35 Ft+	Beculty		- 31
<b>3</b> 4/18/C	2.06.03 Ftv	Beculty		- 21
<b>3</b> ,4/18/0	2.06.03 Ftv	Security.	The second second second	- 23
<b>X</b> 4/18/C	.59.32 Abi	Beculty	Соко Пломогия Пема Воф	
<u>\$</u> ,4/18∕C	.59.32 AM	Becchy.		•

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

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 Domain: %3

Caller User Name: %5

Caller Logon ID: %7

Event ID: 633

Type: Success Audit
Description: Global Group Member Removed:

Member: %1

Target Domain: %3

Caller User Name: %5

Caller Domain: %3

Caller User Name: %5

Caller Domain: %6

Caller Logon ID: %7

Privileges: %8
```

New user accounts:

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

Caller User Name: %4 Caller Logon ID: %6

### 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.

Event Vie	wer-Sacurity Log actine p	) on NSANSLAD					
Huh:	linna	Source:	Calogory	Execut	Harr	Dampader	
<b>Q</b> 419(01	2:22.24 PM	Sec. y	Pi vilogo Upe	570	Administrato	<ul> <li>SANGLAD</li> </ul>	
419,01	2:2211 PM	Sec. ý	Pi viloĝo Use	570	Administrato	r SaNGLAD	1
Q 4/19/CI	2:21 CL FM	Sec. 👽	Detailed Trac in		<ul> <li>Administrato</li> </ul>		
4/19/01	2:21 - S FM	Geo. ty	Object Access	560	Administrato		
4,19,01	2.2179 PM	Section	Oble <u>tanie</u>	562	SUSTEM	SONR 68	
<b>Q</b> 4/19/01	2.2179 PM	Selling	Oble Event Data	1			8
4/19/CI	2.21 +9 PM	Selling	Oble				
<b>Q</b> 4/19/01	2.21 ×9 PM	Selling	Obe bae	40.00	Lo	e9 D - 56.	
% 4/19/CT	2.21 ×8 PM	Selvin	Dep Time	2.2 A3 FH	- Su	ure Sacry	
<b>%</b> 47901	2.2144196	Second	Obel Haa	Auferini de M	• To	an Burn to Au B	
🔍 4/19/4 1	5.7144198	Sec. 2 Million	Other Computer	SANSLAS.	Ca	tecta, ElleviAceter	
41911	25/142198/	Setury	Ohe .				
<b>L</b> 4790 1	25/142198/	Setury	Dhe Broups				
<u>(</u> 479.11	22140 FM	Set. y	Othe	Cinier: Sera			- L
47371	22140 FM	Set. y	e út	Uplec: I (pel Culou Nurr		CATAGORI IN LINE	
47811	22140 FM	Set. y	060	have been			
<u>4,478</u> ,71	224103 FM	Hor. Y	Oho	Costalion D	> លេខ.ឈ.2		
4.19.11	22105 PM	Set. Y	Oho	Fideces I.C.	21:621:25	3	
<b>1,</b> 419,01	2:21 CC PM	Sec. y	Obje	Frie o isas Friez Con		n rv	
<b>Q</b> ANSCI	2:21 CC FM	Sec. ý	)bje	l megulos:			
419CI	2:21 CC FM	Sec. 🔬	)bje	Cler (U., i)			
419.01	2.21 35 PM	Selling			u ta ca		
41901	2.21 27 PM	Sellinia	Dbe Pata 1	Bis C	Weige		
4/19/CI	2.21 27 PM	Selling	Obe				<u></u>
Q 4/19/CT −	2.21 27 PM	Selling	Profil III				Q1 0
¥1901	2.21 27 PM	Selvin	Profil III				01.0
€4/I9/CI	2.07 52 PM	Selvin	Profil III				EL L
Q.47901	5 D/05 PM	SH LOW	Obe 1				1.1
្តីស៊ុះស៊ុះ។	5.1755.196	SH CV	Obe				
•I				NA .	Energia de	No. The	J

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.

res i

	anei - Securițe Lo, Obligită - Leo	g on WSANSLAU					
		Source	Category.	Event	llear	Computer	
Date 4 (19.01) 4 (19	Time 27:340 PM 27:305 PM 27:305 PM 27:300 PM 24:300 PM 24:30	Source Succey Sourcey	Ocjery, Ocjery, Ocjery, Ocjery, Ocjery, Ocjery, Ocjery, Ocjery, Ocjery,	icos 200 icos 2	Mic A rator 18 I 19 I 19 I 19 I 19 I 19 I 19 I 19 I 19	SANGLAE SANGLAE SANGLAE SANGLAE SANGLAE SANGLAE SANGLAE SANGLAE SANGLAE SANGLAE SANGLAE SANGLAE SANGLAE SANGLAE SANGLAE SANGLAE SANGLAE SANGLAE	N 0000000 N
ଷ୍ଟ ଏମଥର 1 ଷ୍ଟ୍ର ଏମଥର 1 ଷ୍ଟ୍ର ଏମଥର 1 ଷ୍ଟ୍ର ଏମଥର 1 ଷ୍ଟ୍ର ଏମଥର 1	24001 - 94 24321 - 94 24321 - 94 24321 - 94 243219 - 94 243219 - 94	Kenuriy Becuriy Becuriy Becuriy Becuriy	Ocjent Ocjent Ocjent Privitec Privitec	ign @ Bee	C gab		Å
				<u></u>	Levor	Beal   Let:	

Figure 25: Event ID 564 Object Delete Handle ID

Date	_pacns _eo Llinne	Source	Gategory	L vent	User	Gamputer	
<u>, 17 9</u> (01	213,40 PM	Scorte	Prvilugu Uuv	578	Adminicast.		
Q () 201 -	2 - 3,35 PM	Subarto	Dboll Acces	Ē62	Adminicas).		
Q., 201	2 - 3,33 PM	Subrty	Dboll Access	562	Adminicas).		
Q ( 20)	213.33 PM	Subrty	Dboll Access	560	Adminicas).		
🤹 ( a) ( i	2 - 3,33 PM	Subarto	Dourace.	E62	Adminita et.		
Q ( 20)	2 - 3,33 PM	Subarto	Dourace.	E6-1		I SANSLAE	
- 10 a 01	21333 PM	Scourte	Oblet. Access	560		I SANSLAE	
<b>Q</b> (*) 3(01	2 43.32 Trid	Security	Oble	664		. 54.61 AE	
🕻 🖓 3(0) -	2 43.32 754	Securio	Obel, Eventi	letel			
Q ( 30)	2 +3.27 TVI	Securio	Oble_				
Q (* 30)	2 +3.27 TVI	Securio	Obel Cou	4/19/0		E-vr.10. 060	
Q (* 30)	2 +3.27 TVI	Securio	Obel, Inc.	1:1331	19	Source Lecuity	
<b>1</b> (1) 3(2)	2 + 3,26 Trid	Securio	Obel _wat	ACTIVIC:	excr	yox cocess wet	
🤹 ( 3,0) -	2 +3.24 TM	Securio	Obel Doc	uter: CANSLA	£	Estegory: Object modess.	
🤹 (j. 201	2 43.24 754	Security	Obles. Sec.				
🤹 (j. 201	2 43.24 754	Security	21.00				
Q ( 30)	2 43.24 754	Security	Oble. 14	մ Դրեր Դիլեր Դ	er-on Teruñ	_	
N + 301	2 43.24 TM	Security	Obel.	Jbject		?	
N 9 301	2 43.24 TM	Security	Obel.	06.01		ni waki aku ya kup	
N 9 301	2 43.24 TM	Security	Obel.	New La			
10£ 0	2 +3.24 TM	Securio	Obel.	Uperation			
(4) 301	243.21 754	Securio	Obel.	ກັບແກດ ອີກັນສະມີ		(415 : 140	
10£ 0	243.21 754	Securio	Obel.	hina, L			
ર્ય તેમાં ન	245.21 PM	Securio	Obel.		ogen up (Malle		
ર્ય તેમાં ન	245.21 PM	Securio	Obel.	@ <u>1</u> ,00	C Small		
ર્ય તેમાં ન	242.21 194	Securio	Obel.	6. 200	- <u></u>		_
Ne Riji	24021 24	Securio	Obel.				
ເຈົ້າ ເປັນ	24219 24	Securio	Trailed 1				
N (n	24-19-24	Security	trud-a				
							ШE

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*.

	_pach;ep	0	0	In		0	
)ate	Time	Source	Category	Event	User	Camputer	
<u>4</u>	3 05.33 PM	Secure	Oblet. Access	560	Administration		
<u>, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10</u>	3 05.33 PM	Security	Oblet, Access	560		JI EANELAE	
47 3(01	3 05.33 TM	Security	Depres Trocki	9592		a EANSLAE	
( N 301	8 CE.22 TM	Securio	Deta Fyent Det		1 haini 1 d	. FALCINE	2
<u>रितिकम्</u> याः	317.58 M	Securio	260	лı			-
<u>1974</u>	24 (40 ) NA	Secondy.	in sala Ditana 19400	4219201		-endlig 650	
947 <del>1</del> 1	2.4 · 35 · 24	Secondy.		2000 C		nan da seconda Nace - Seconda	
14140	24 - 33 PM	Secondy Controls		- Carnin - Dala		rana seranas Ale Sulasekolun I	
147 A.U.	2.4 - 33 PM	Security Manual		SCN5 AB		aren 1911 betailen Treckin	
147 A H	2,4 -33, PM 2,4 -33, PM	Mercurity Marking	tabi au	100 m		e en y trenden neux a	
(421-0) (221-0)	2.4 - 33 - 54 2.4 - 33 - 54	Mercurity Mark the		••			
(4) (0 U	2.4 - 32 - 54	Mercurity Marcuri	Uhlei Andvio	ocess kas de			<b>A</b>
(२१२) स्थाः (२११ स्थाः	2.4 (32 - 54	Menuely Menuely	Uher Comme	H & Put p			
147.40	7 - 17 - M	Secury	Dihjer Dihjer	Inege Field	erse – HISTRAG Jese Lie 2062 JUN		
147.41	2 - 27 - 3	Secury	Dhe:	User Narra			
14.60	2 - 27 - 3	Seculy	Dher	Date - Anton	SCHADE	RT .	
14.40	2 4 126 -134	Seculy	Dher	Logen 20	TURAU LI ACI	(32.,	
12.40	21.24-34	Secuely 19	Other				
the an	21.24-34	Secury	Other				A0000003
e de m	21.24-34	Secuely 1	table a	e.			
ંગવેલાં	21724 - 4	Seculy	Oho: Date (	Sight C	≝aa		
¢ ý à01 -	210:24 PM	Security	Oble:				ŝ
V 201	2 10:24 PM	Security	Object				
V 901	2 10:24 PM	Sec. ity	Obje:				
( / a/01	2 0:24 FM	Secury	Obje:				
( ) a(01	2 0:21 FM	Secury	0bje: ∢				CD-I
10,6 1	2 0:21 FM	Scc. ( b)	Obje:				
( ) ajor	2 0:21 FM	Scc. ( b)		he	Fowirus	Net Help	

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.

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. a.

### References

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

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

Sutton, Stephen A., <u>Windows NT Security Guide</u>. 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).

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