Using Event Logs to Audit Windows NT4

Practical Assignment for
SANS GIAC Training
Securing Windows NT
Ottawa Ontario Canada
August 2000

Howard F. Gabert, P.Eng.

Table of Contents:

Overview:

With the growth of the Internet and expansion of worldwide communication, there is increasing urgency to tighten security and to carefully monitor use of computers and networks. As networks grow, more computers are interconnected, all which become potential targets. Hackers and crackers could exploit any system vulnerability left unprotected as they pursue their intentions of denying or disrupting service, or attempt to steal or compromise sensitive information.

Security planning involves various levels of protection, including perimeter protection and firewalls, controlled physical access to servers and workstations, careful management of user accounts and passwords, and effective deployment of software patches and updates. Auditing can be deployed to evaluate the success of these defenses, to detect whether various security measures have been circumvented, and to evaluate to what extent any exploitation has been successful. Analysis of the audited data can assist in determining what security settings need to be changed to deny the violation. By using auditing to study the offensive attack, better defensive techniques can be deployed.

Simply stated, auditing is a process that generates and records data related to various activities controlled by the operating system. By selecting which activities are recorded, auditing can be used to detect abuse or misuse of computer systems as well as general information about system use. Since auditing can be used to detect intrusions, the audit system will also be subject to attack. The intruder may attempt to disable auditing, modify the audit logs to erase evidence, flush or destroy the audit logs. Therefore the event logs themselves must be protected.

Windows NT server and NT workstation have common security architecture, providing a basic set of features that is consistent across both platforms. The operating system and NTFS file system were designed to generate useful auditing information. Note that other applications such as Microsoft Internet Information Server and Microsoft Exchange server also generate event logs: those logs will not be included in this discussion.

Audited Events:

Windows NT can record a variety of event types. These include events such as user login, file access and process tracking. Windows NT can also audit when any of the user rights are granted to a user or group. Both successful and unsuccessful attempts to perform any action can be recorded.

There are seven basic event types in Windows NT. Collecting data related to each event type can be enabled or disabled. Since auditing uses system resources and generates overhead, careful selection of which events are recorded is desirable. Selection requires an understanding of the event types and whether they would provide useful information if enabled. Brief descriptions of the event types follow:

- Login and Logoff - These events describe login and logoff attempts, whether successful or unsuccessful, and a description of the login type (interactive, network or service).
- File and Object Access - These events describe both successful and unsuccessful access to protected files, folders, printers and other objects..
- Use of User Rights - These events describe successful and unsuccessful attempts to use privileges.
- User and Group Management - These events describe changes to the user accounts database such as the creation, modification and deletion of users and groups, including account disabling and password changes.
- Security Policy Changes - These events describe changes made to user rights, security policy database and trust relationship policy.
- Restart, Shutdown and System - These events describe system restarts and shutdown and events that affect system security or the security event log.
- Process Tracking - These events describe program activation, handle duplication, indirect object accesses, and process exist.

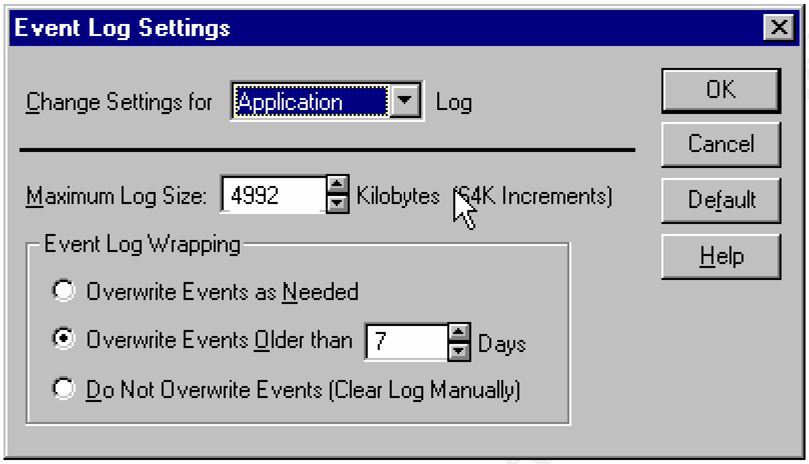
Configuration of Event Logging:

Auditing is disabled following a default installation of Windows NT. Before auditing is enabled, the log and archival process should be properly configured. If the service is started and then a configuration setting is changed, that change may not be applied immediately. For example, if the log size is changed after logging is enabled, the change in size does not take place immediately. After changing the size you will be asked if you wish to save the file. After answering this question, you must then clear the log before the change in log size takes place. Unfortunately this will cause all history saved in that log to be lost.

Log settings are configured using the ***Event Viewer***. Start ***Event Viewer*** and open ***Log Settings*** under ***Log***. Here you can change settings for the Application, System and Security log. As NT records events in a log file, the log file grows until it reaches the specified maximum size. When the maximum size is reached, you can specify what action will occur.

- Overwrite Events as Needed - As maximum log size is reached, the oldest events will be discarded and overwritten. This setting can be weak in circumstances where programs trap into infinite loops resulting in a flood of events. The resulting log will be full of identical events and the precipitating cause will not be saved.
- Do Not Overwrite Events (Clear Log Manually) - As maximum log size is reached, NT will stop recording events until the log is manually cleared. This setting is weak as once the log is full, you must clear the log and all history is lost.
- Overwrite Events Older than X Days - As maximum log size is reached, NT discards events older than the number of days specified. If the log becomes full

of events younger than the specified days, NT stops recording until other events expire. This may be the best choice in many environments, particularly if logs are copied to a remote location on a regular basis.



Change Settings for Application Log

Maximum Log Size: 4992 Kilobytes (64K Increments)

Event Log Wrapping

○ Overwrite Events as Needed

● Overwrite Events Older than 7 Days

○ Do Not Overwrite Events (Clear Log Manually)

No matter how the settings are configured, it is possible to lose events if the system is flooded with events that must be recorded in the log. The maximum log size should be made reasonably large to avoid short-term problems, and sufficiently large to store data for several days of operation. The amount of log space required depends on the activity level, the number of events enabled for auditing, and the level of object auditing in use. For example, if one observes that a particular log file grows by 2Mb in a week, and if the logs are regularly copied to a central server once a week, then by setting the maximum log size to 8Mb, a reasonable safety margin is established.

One other possible action can occur when the security log file space is full. The action is called ***CrashOnAuditFail***. ***CrashOnAuditFail*** will cause the system to stop only when the security log is filled, and has no affect on system operation when the application or system log is filled. To enable, edit the registry key ***CrashOnAuditFail*** setting the value to 1 which will cause the system to halt with a ***STOP*** message and a blue screen when the security log is filled.

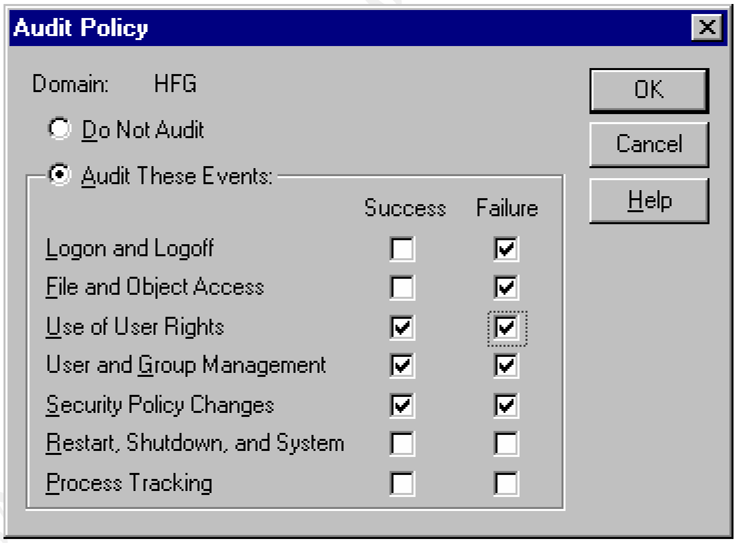
Hive: HKEY_LOCAL_MACHINE
Key: SYSTEM\CurrentControlSet\Control\LSA
Name: CrashOnAuditFail
Type: REG_DWORD
Value: 1

Just before the system is halted, the operating system changes the key's value to 2, indicating that when the system is restarted, only an account belonging to the Administrators group may initially log on. Changing the key's value back to 1 enables normal login sessions. The system must be restarted each time the ***CrashOnAuditFail*** value is changed. The only way to disable this feature is to delete the key from the registry.

Strategies to archive logs are necessary to maintain long enough histories to detect and isolate security violations that have been ongoing for an unknown period. Every NT system has its own set of logs consisting of events recorded by that system. These local logs are only a partial view of the enterprise, and analysis of enterprise security will require analysis of logs from more than one system. The analysis of logs from many computers is more easily accomplished if the logs are all collected in one location. Various tools are available to copy the logs to a central location, a task that should be scheduled on a weekly or daily basis to ensure that adequate historical information is retained. Examples of these tools appear later.

Enabling Auditing:

Following a default installation of Windows NT, auditing is disabled. Once auditing is configured, auditing must be enabled. This is done by running the ***User Manager*** and selecting ***Audit*** under ***Policies***. Success or failure for each of the seven event types can be selected.



Domain: HFG

○ Do Not Audit

● Audit These Events:

	Success	Failure
Logon and Logoff	□	☑
File and Object Access	□	☑
Use of User Rights	☑	☑
User and Group Management	☑	☑
Security Policy Changes	☑	☑
Restart, Shutdown, and System	□	□
Process Tracking	□	□

Note that audit policy set on an NT workstation, server or stand-alone system applies only to that system, whereas an audit policy applied to a domain controller applies to all domain controllers.

NT Event Log Files:

Windows NT generates three event logs.

- **APPEVENT.EVT** - Application Event Log - Records user application events, and events related to system processes
- **SYSEVENT.EVT** - System Event Log - Records events logged by NT system services, drivers and kernel mode events
- **SECEVENT.EVT** - Security Event Log - Records Windows NT security and system auditing events

The three log files are saved in ***%SYSTEMROOT%\SYSTEM32\CONFIG\*** with .EVT extensions. The location of these files is not configurable.

By default, guests and unauthorized users can read the System and Application event logs. To limit access to authenticated users, edit the following registry keys.

> Hive: HKEY_LOCAL_MACHINE
> Key: SYSTEM\CurrentControlSet\Services\EventLog\Application
> Name: RestrictGuestAccess
> Type: REG_DWORD
> Value: 1 Restrict access to Application log

> Hive: HKEY_LOCAL_MACHINE
> Key: SYSTEM\CurrentControlSet\Services\EventLog\System
> Name: RestrictGuestAccess
> Type: REG_DWORD
> Value: 1 Restrict access Event log

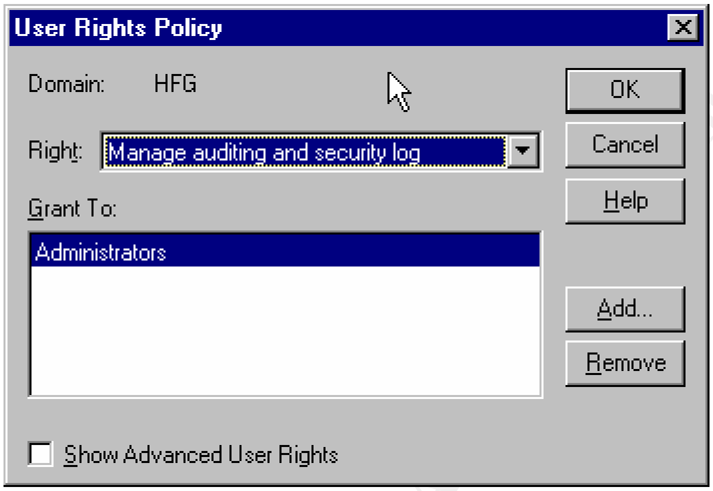
Note that guests and unauthorized users cannot read the Security event log. However, if the same action is taken for the Security log, then the security log will be also be secured for anyone who has been assigned the ***Manage auditing and security log*** user right.

The event logs can also be assigned access rights to limit the users who can read the files. By default, ***Everyone*** is able to read these files. The access rights should be edited to remove ***Everyone*** and to restrict access to members of the ***Administrators*** and ***System*** groups.

- Using Windows NT Explorer, highlight an event log file, select ***File***, ***Properties***, click on the ***Security*** tab and then click on the ***Permissions*** button
- Use the ***Remove*** button to remove the ***Everyone*** group.
- Click the ***Add*** button and then double-click to add ***Administrators*** and ***SYSTEM***. Then click ***OK***.
- Set the ***Type of Access*** for ***Administrators*** and ***SYSTEM*** to, ***Full Control***. Then click ***OK***.
- Repeat the above steps for each of the log files.

As an additional security measure, access to the log files could be audited for all types of access. However, avoid logging access by the System account to the log files as this will generate unnecessary overhead.

The ***User Rights Policy*** includes a right that allows a user to configure SACLS on folders, files and registry keys, and to view and clear the security log. This right should only be assigned to the Administrators group, or selected users when necessary. To configure, open ***User Manager***, select ***User Rights*** under ***Policies***, and then select ***Manager auditing and security log*** under the pulldown menu in ***User Rights Policy***.


User Rights Policy

Domain: HFG

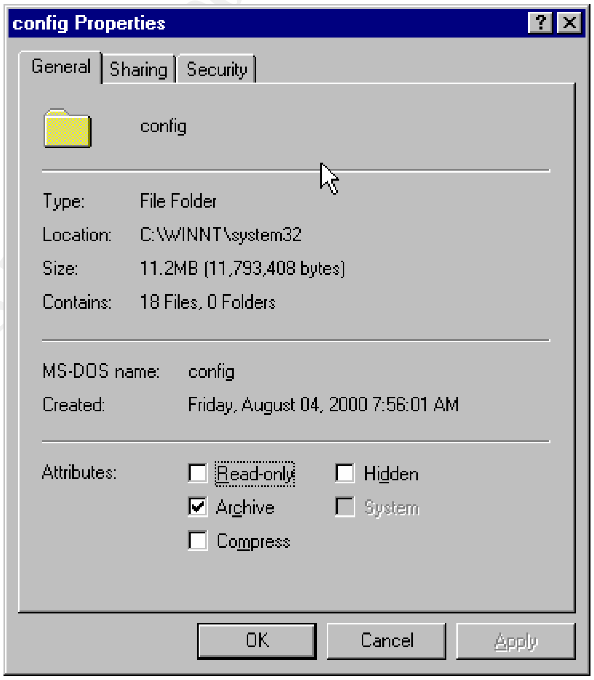
Right: Manage auditing and security log

Grant To:

Administrators

□ Show Advanced User Rights

If ***File and Object Access*** is enabled, you also need to configure the files, directories, printers and register settings that are to be audited. To enable auditing on a file, folder or printer, open ***Windows NT Explorer***, highlight the file, directory or printer you want to change and then select ***Properties***.


config Properties

config

Type: File Folder

Location: C:\WINNT\system32

Size: 11.2MB (11,793,408 bytes)

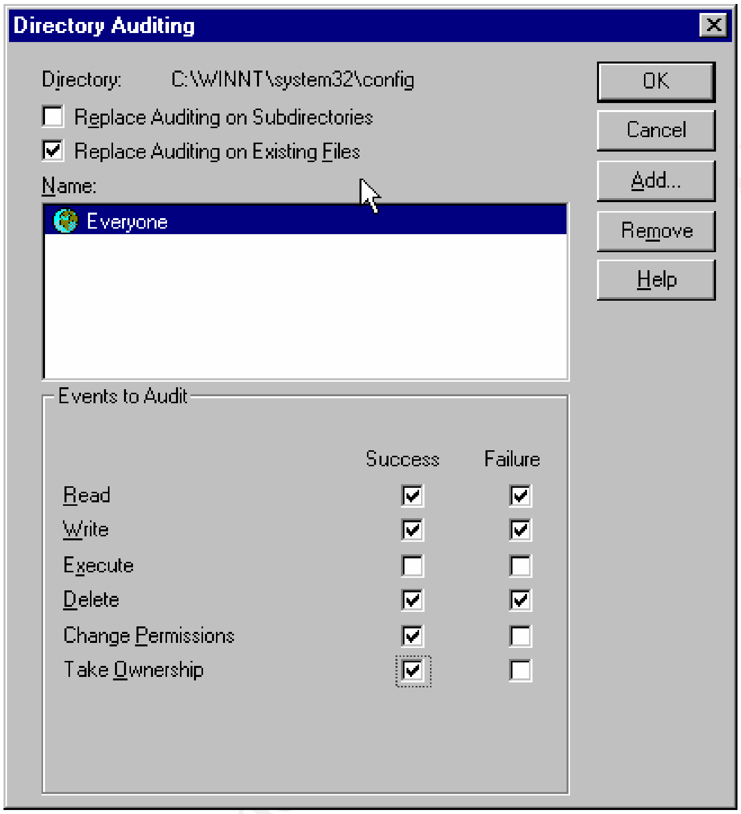
Contains: 18 Files, 0 Folders

MS-DOS name: config

Created: Friday, August 04, 2000 7:56:01 AM

Attributes: □ Read-only □ Hidden ☑ Archive □ System □ Compress

Next select ***Security*** and then ***Audit***. Select the actions that are to be audited for that item. When enabling or changing auditing on a directory, you can also chose to deploy the same settings on subdirectories and existing files.



Directory Auditing

Directory: C:\WINNT\system32\config

☐ Replace Auditing on Subdirectories

☑ Replace Auditing on Existing Files

Name:

Everyone

Events to Audit

	Success	Failure
Read	☑	☑
Write	☑	☑
Execute	☐	☐
Delete	☑	☑
Change Permissions	☑	☐
Take Ownership	☑	☐

To enable or change auditing on registry entries, use ***REGEDT32***. Open the registry key that is to be audited, click on ***Security***, then ***Auditing*** and select what actions are to be recorded in the event logs.

Auditing Deployment Across the Enterprise:

The ***User Manager*** on servers and the ***User Manager*** on workstations can be used to customize auditing. Deployment of an NT Audit policy across the enterprise requires that the policy be applied consistently and accurately on each system. This can be accomplished by visiting every workstation individually, but this is time consuming and prone to errors while trying to replicate a standard group of settings. Some of the tools that will be described shortly have to the ability to unify audit policy and log settings across the enterprise, configuring multiple workstations in the network from a central console. Consistent policy and consistent log settings are required to ensure that sufficient data is collected in the logs.

Tools to Archive and Examine Logs:

Event Viewer is the only tool provided with Windows NT to access and view the event logs. Whereas ***Event Viewer*** can be used to access logs on remote computers, this tool is inadequate for performing analysis and archiving of logs.

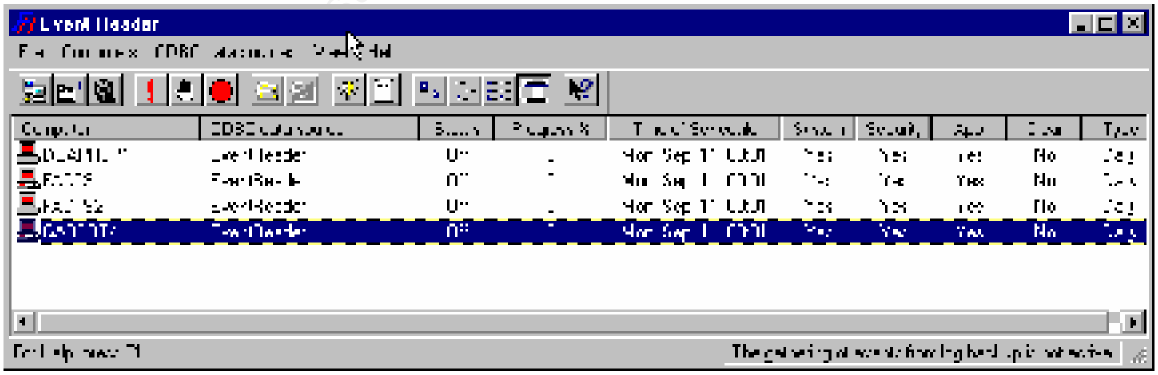
The SANS course ***Securing Windows NT*** examines the applications ***DUMPEL*** (Microsoft NT Resource Kit), ***DUMPEVT*** (http://www.somarsoft.com), ***EVNTSLOG*** and ***NTSLOG*** (http://www.adiscon.com). The course material also examines third-party applications ***BindView*** (http://www.bindview.com), ***Event Log Monitor*** (http://www.systemtools.com/elm), and Aelita ***EventAdmin*** (http://www.aelita.net). Discussion of these utilities will not be repeated here. Instead several other archiving and monitoring tools will be examined.

EventReader:

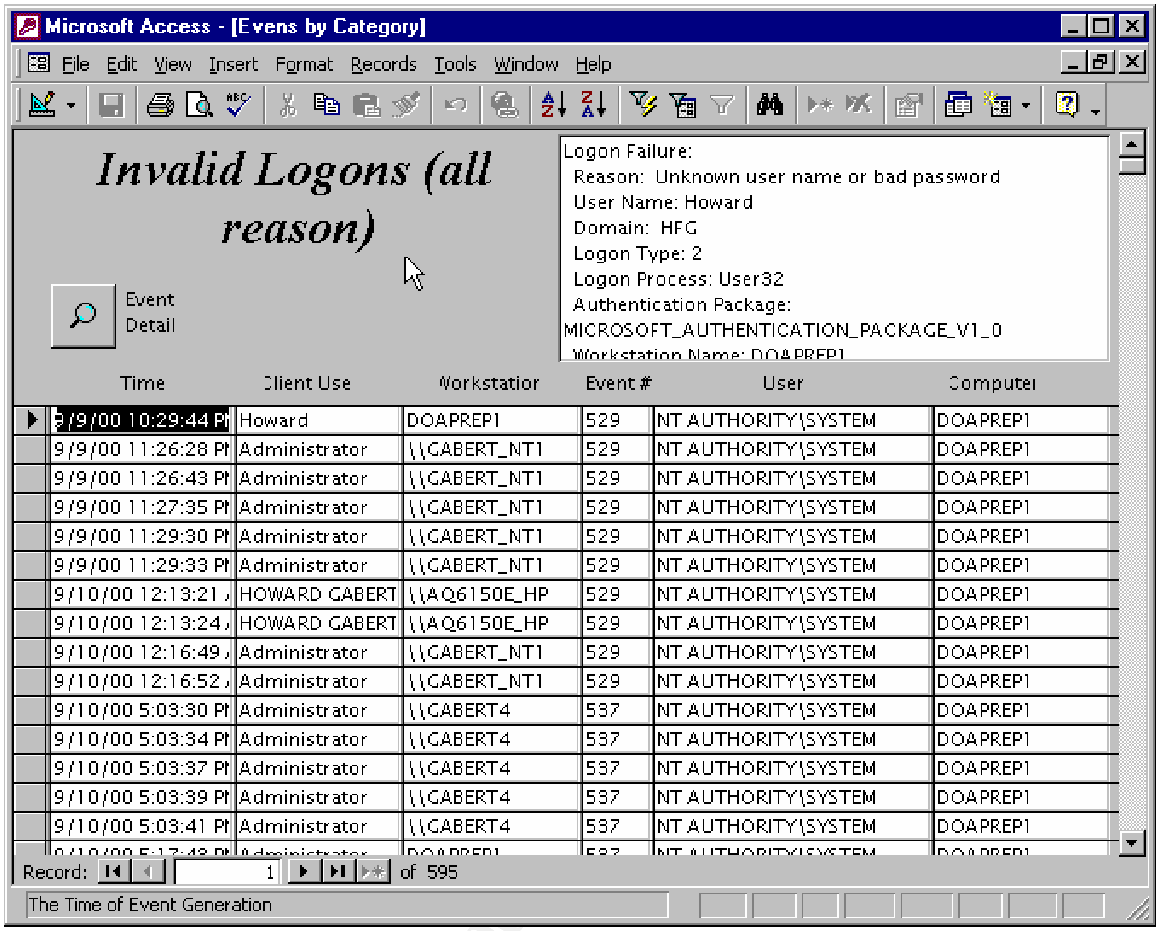
http://www.strongsoftware.net/eventrd/

EventReader is an administrative tool that will collect event logs from Windows NT computers in a network, storing the data in a central ODBC compatible database. The central collection of data from all systems enables analysis of complex situations where multiple computers are involved in an event. Centralized data collection also provides additional security for the log event files and the opportunity to backup and save the logs to preserve history.

EventReader includes a sample ***MS Access 8.0*** sample database. ***EventReader*** is configured to collect data from specific computers in the network according to a collection schedule.



EventReader also provides tools to assist in analyzing the logs. Data is sent to an ***ODBC*** database when collected. The sample ***Access*** database includes analysis of the logs to detect various conditions. A sample of the login failure summary appears below.


Microsoft Access - [Evens by Category]
File Edit View Insert Format Records Tools Window Help

Invalid Logons (all reason)

Logon Failure:
 Reason: Unknown user name or bad password
 User Name: Howard
 Domain: HFG
 Logon Type: 2
 Logon Process: User32
 Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
 Workstation Name: DOAPREP1

Time	Client Use	Workstation	Event #	User	Computer
9/9/00 10:29:44 Pl	Howard	DOAPREP1	529	NT AUTHORITY\SYSTEM	DOAPREP1
9/9/00 11:26:28 Pl	Administrator	\\GABERT_NT1	529	NT AUTHORITY\SYSTEM	DOAPREP1
9/9/00 11:26:43 Pl	Administrator	\\GABERT_NT1	529	NT AUTHORITY\SYSTEM	DOAPREP1
9/9/00 11:27:35 Pl	Administrator	\\GABERT_NT1	529	NT AUTHORITY\SYSTEM	DOAPREP1
9/9/00 11:29:30 Pl	Administrator	\\GABERT_NT1	529	NT AUTHORITY\SYSTEM	DOAPREP1
9/9/00 11:29:33 Pl	Administrator	\\GABERT_NT1	529	NT AUTHORITY\SYSTEM	DOAPREP1
9/10/00 12:13:21 /	HOWARD GABERT	\\AQ6150E_HP	529	NT AUTHORITY\SYSTEM	DOAPREP1
9/10/00 12:13:24 /	HOWARD GABERT	\\AQ6150E_HP	529	NT AUTHORITY\SYSTEM	DOAPREP1
9/10/00 12:16:49 /	Administrator	\\GABERT_NT1	529	NT AUTHORITY\SYSTEM	DOAPREP1
9/10/00 12:16:52 /	Administrator	\\GABERT_NT1	529	NT AUTHORITY\SYSTEM	DOAPREP1
9/10/00 5:03:30 Pl	Administrator	\\GABERT4	537	NT AUTHORITY\SYSTEM	DOAPREP1
9/10/00 5:03:34 Pl	Administrator	\\GABERT4	537	NT AUTHORITY\SYSTEM	DOAPREP1
9/10/00 5:03:37 Pl	Administrator	\\GABERT4	537	NT AUTHORITY\SYSTEM	DOAPREP1
9/10/00 5:03:39 Pl	Administrator	\\GABERT4	537	NT AUTHORITY\SYSTEM	DOAPREP1
9/10/00 5:03:41 Pl	Administrator	\\GABERT4	537	NT AUTHORITY\SYSTEM	DOAPREP1
9/10/00 5:17:43 Pl	Administrator	DOAPREP1	537	NT AUTHORITY\SYSTEM	DOAPREP1

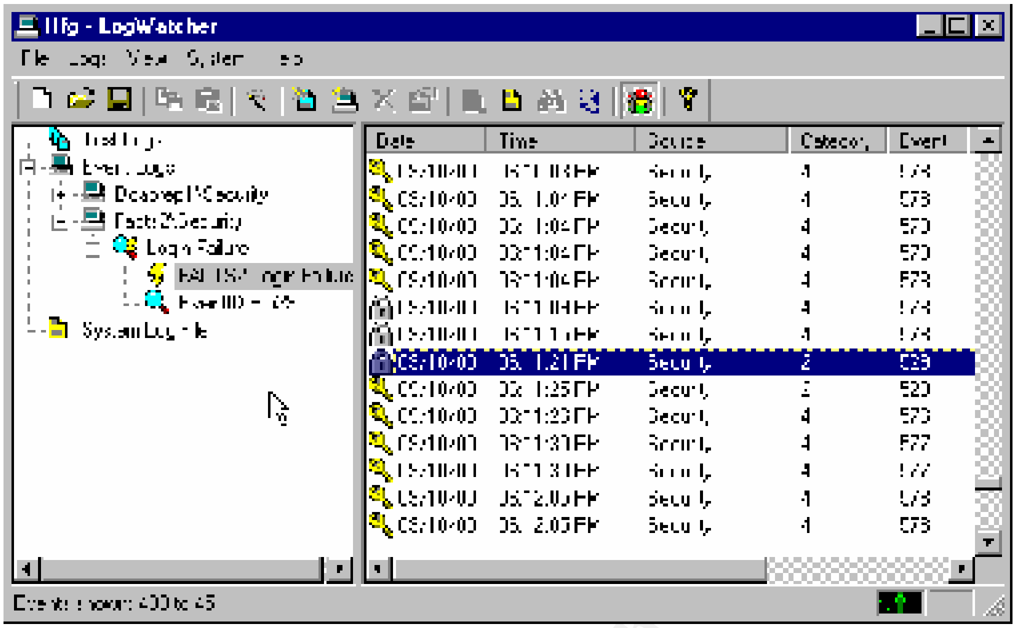
Record: 1 of 595

The Time of Event Generation

LogWatcher:

http://www.acrasoft.com

LogWatcher 1.0 is a utility designed to search through Windows NT event logs to find certain keys that you define, and to execute special tasks when it finds them. For example, login failures due to unknown user name or bad password would be detected by watching for security log event 529.

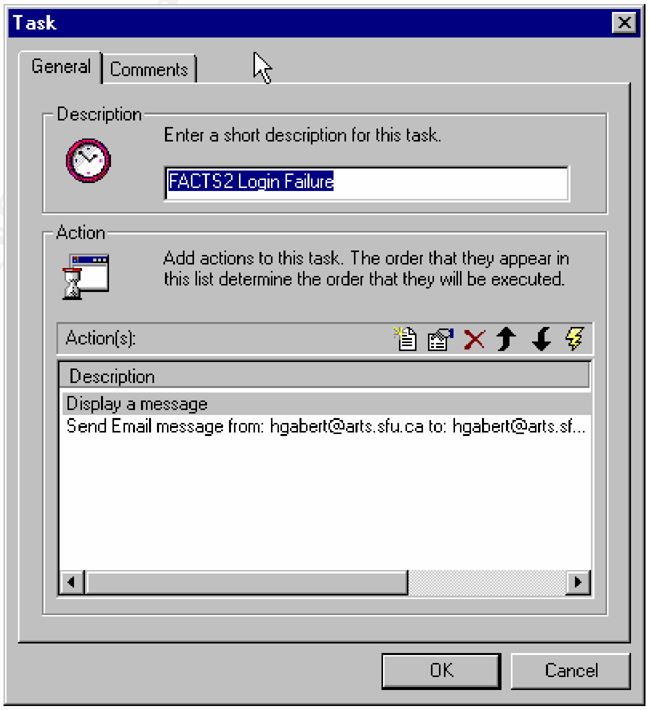


Date	Time	Source	Category	Event
[illegible]	[illegible]	Security	4	529
05/10/00	05: 1.07 PM	Security	4	529
05/10/00	05: 1:04 PM	Security	4	529
05/10/00	05: 1:04 PM	Security	4	529
05/10/00	05: 1:04 PM	Security	4	529
[illegible]	[illegible]	Security	4	529
[illegible]	[illegible]	Security	4	529
05/10/00	05: 1.21 PM	Security	2	539
05/10/00	05: 1:25 PM	Security	2	529
05/10/00	05: 1:29 PM	Security	4	529
05/10/00	05: 1:31 PM	Security	4	529
[illegible]	[illegible]	Security	4	529
05/10/00	05: 2.05 PM	Security	4	529
05/10/00	05: 2.05 PM	Security	4	529

Events shown: 400 to 45

LogWatcher will search logs on multiple remote computers, and will examine the event logs on those machines for specified fields and values you want. Event logs will be examined for the defined events at a sample interval time configured for each computer. The default sampling interval is set to 60 seconds.

When events are detected, ***LogWatcher*** can be configured to take various actions such as sending e-mail or displaying a message. These notifications can alert Administrators to particular events as they occur. The sample screen below shows that detection of event 529 in the security log will result in notification by e-mail and a pop-up message window.



Description

Enter a short description for this task.

FACTS2 Login Failure

Action

Add actions to this task. The order that they appear in this list determine the order that they will be executed.

Action(s):

Description
Display a message
Send Email message from: hgabert@arts.sfu.ca to: hgabert@arts.sf...

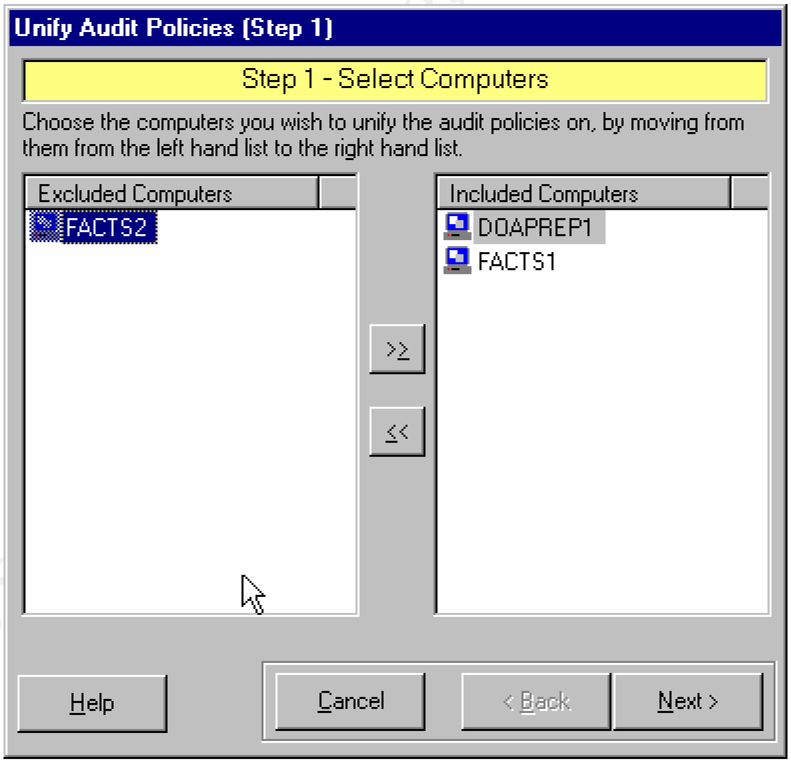
LogWatcher is not the best utility to archive and backup logs for the enterprise. But the dynamic examination of logs with programmable actions upon detection is extremely useful in sending notification when security violations occur. ***LogWatcher*** is a very useful tool to detect when a particular event or security violation is occurring, providing timely notification enabling quick action to find the offender.

Event Archiver Enterprise:

http://www.doriansoft.com/eventarchiver/index.htm

Event Archiver Enterprise can be configured to collect logs from remote computers, storing the logs in a central location. ***Event Archiver Enterprise*** does not need client software on each computer. A single console on a central computer can manage the event logs across multiple domains.

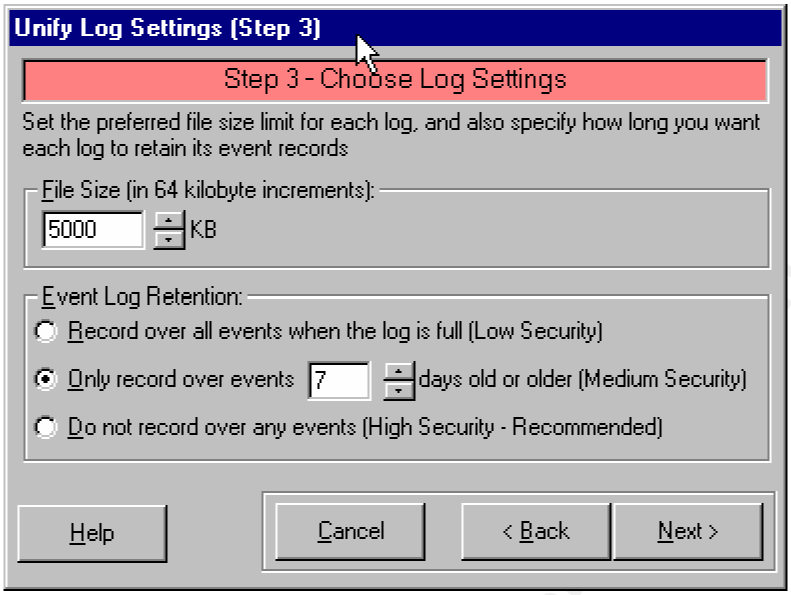
Event Archiver also provides tool wizards to unify audit policies across selected computers.



Choose the computers you wish to unify the audit policies on, by moving from them from the left hand list to the right hand list.

Excluded Computers	Included Computers
FACTS2	DOAPREP1
	FACTS1

Event Archiver also provides a tool wizard to unify log settings across selected computers on the network.



Unify Log Settings (Step 3)

Step 3 - Choose Log Settings

Set the preferred file size limit for each log, and also specify how long you want each log to retain its event records

File Size (in 64 kilobyte increments): 5000 KB

Event Log Retention:

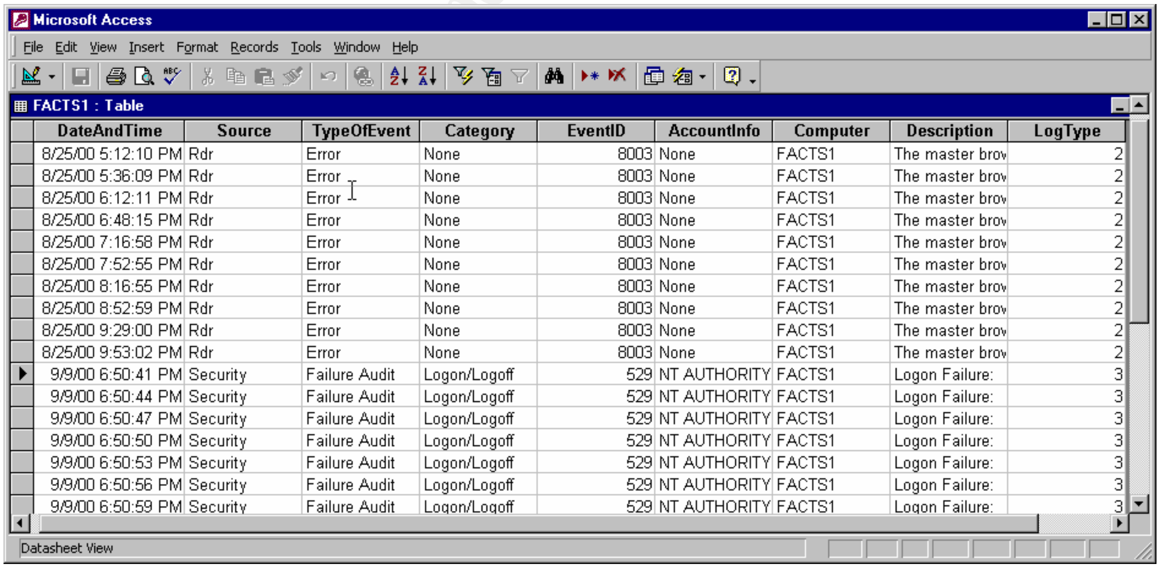
○ Record over all events when the log is full (Low Security)

● Only record over events 7 days old or older (Medium Security)

○ Do not record over any events (High Security - Recommended)

Both of these features simplify management and reduce the cost of auditing. By having consistent log settings and audit settings, Administrators can be certain that the proper events are being recorded.

Event logs from remote computers can be moved and archived on a single console. Data can be directly saved into ***Access*** or ***SQL*** server databases. Data collection can occur daily, weekly, or when the logs reach a certain size. A sample ***Access*** database log view appears below.



FACTS1 : Table

DateAndTime	Source	TypeOfEvent	Category	EventID	AccountInfo	Computer	Description	LogType
8/25/00 5:12:10 PM	Rdr	Error	None	8003	None	FACTS1	The master brov	2
8/25/00 5:36:09 PM	Rdr	Error	None	8003	None	FACTS1	The master brov	2
8/25/00 6:12:11 PM	Rdr	Error	None	8003	None	FACTS1	The master brov	2
8/25/00 6:48:15 PM	Rdr	Error	None	8003	None	FACTS1	The master brov	2
8/25/00 7:16:58 PM	Rdr	Error	None	8003	None	FACTS1	The master brov	2
8/25/00 7:52:55 PM	Rdr	Error	None	8003	None	FACTS1	The master brov	2
8/25/00 8:16:55 PM	Rdr	Error	None	8003	None	FACTS1	The master brov	2
8/25/00 8:52:59 PM	Rdr	Error	None	8003	None	FACTS1	The master brov	2
8/25/00 9:29:00 PM	Rdr	Error	None	8003	None	FACTS1	The master brov	2
8/25/00 9:53:02 PM	Rdr	Error	None	8003	None	FACTS1	The master brov	2
9/9/00 6:50:41 PM	Security	Failure Audit	Logon/Logoff	529	NT AUTHORITY	FACTS1	Logon Failure:	3
9/9/00 6:50:44 PM	Security	Failure Audit	Logon/Logoff	529	NT AUTHORITY	FACTS1	Logon Failure:	3
9/9/00 6:50:47 PM	Security	Failure Audit	Logon/Logoff	529	NT AUTHORITY	FACTS1	Logon Failure:	3
9/9/00 6:50:50 PM	Security	Failure Audit	Logon/Logoff	529	NT AUTHORITY	FACTS1	Logon Failure:	3
9/9/00 6:50:53 PM	Security	Failure Audit	Logon/Logoff	529	NT AUTHORITY	FACTS1	Logon Failure:	3
9/9/00 6:50:56 PM	Security	Failure Audit	Logon/Logoff	529	NT AUTHORITY	FACTS1	Logon Failure:	3
9/9/00 6:50:59 PM	Security	Failure Audit	Logon/Logoff	529	NT AUTHORITY	FACTS1	Logon Failure:	3

Event Archiver provides a complete set of tools to unify audit and log settings, to move logs from distributed computers to a single workstation, and provides an interface to store the logged information of an ***ODBC*** compliant database where log analysis can be configured.

Intrusion Detection:

An intrusion consists of events related to attempts to break into or misuse your system. The word “misuse” is broad and can refer to a severe situation where confidential data is stolen or to a minor situation where an e-mail system is attacked with spam. An intrusion detection system is a system for detecting any kind of "misuse".

Intrusion detection systems (IDS) collect and analyze data which can come from many sources. Systems commonly monitor packets on the network and attempt to discover statistical patterns that indicate a hacker is attempting to break into a system, or the system looks for patterns that match well-known attacks. A typical example is a system that watches for a large number of TCP connection requests (SYN) to many different ports on a target machine, thus discovering if someone is attempting a TCP port scan.

IDS systems may also monitor files and the registry to detect when an intruder changes them. Other IDS systems analyze and use the data found in the event log files, being able to detect when a normal user somehow acquires administrator privileges, when login attempts fail, when attempts are made to change file access rights, or when attempts are made to access restricted files. The signature associated with repeated actions that fail is a strong indicator that an intrusion process is underway.

IDS systems typically provide the following features:

- send automatic notification when an event occurs
- detect and respond to a group of events, called a signature
- analyze and view an aggregate of event logs from multiple computers
- centralized storage and management of log data for multiple computers in the enterprise
- improved query and reporting tools for data analysis

The SANS course material for ***Securing Windows NT*** identified the applications ***RealSecure*** (http://www.iss.net), ***Intruder Alert*** (http://axent.com) and ***CyberSafe*** Centrax (http://www.cybersafe.com) as products that used and analyzed the event logs. There are many other commercial products, and the descriptions of a few follow.

CyberCop:

http://www.nai.com

CyberCop Monitor is a real-time system designed to protect servers. ***CyberCop*** automates the process of detecting intrusions and sends customized automatic responses. For example, if an authorized user attempts to modify content of a file where access is denied, ***CyberCop*** can be configured to logout the intruder and notify the administrator that the attempt occurred, while allowing authorized users continued use of the resource.

CyberCop is designed to detect and attack tampering including unauthorized changes in user privileges, illegal Web site content modification and illegal logins. When intrusions are detected, ***CyperCop*** can be configured to respond in various ways including terminating the offending process, terminating offending login connections, and disabling offending accounts.

CyberCop combines packet analysis with assessment of the event logs, providing an audit trail query and reporting features to document security breaches, suspicious activity, policy violations, and resource utilization, including a record of when intrusions or misuse are detected. Developed under the ***Microsoft Management Console*** user interface, ***CyberCop*** provides an easy to use graphical interface for local or remote reporting, and remote installation. The configuration editor allows for custom settings and thresholds to suit the environment, including security profiles, account groups, time and subnets.

Kane Security Monitor:

http://www.cstl.com/html/info/idi/ksm.htm

The ***Kane Security Monitor*** (***KSM***) is a real-time intrusion detection system designed to protect servers and workstations on the network. ***KSM*** provides enterprise-wide centralized collection of event logs otherwise stored separately on each machine. By automatically reviewing the event logs, KSM searches for patterns of misuse and signatures related to well-known security attacks.

KSM analyzes NT Security event logs on an enterprise-wide basis and is able to continually monitor NT security event logs on thousands of NT servers and workstations. Using artificial intelligence technology, security event logs are scrutinized for abuse patterns including unauthorized activities and suspicious behavior from outside hackers and inside authorized users. This process automatically turns massive amounts of NT security event log data into concise security information.

KSM will send customized alerts when intrusions are detected. However, ***KSM*** is unable to terminate the intrusion or take actions such as logging out the offender. In addition ***KSM*** requires the installation of a software module on the client computers. Notwithstanding these two issues, ***KSM*** is less expensive than some other products and therefore should be evaluated.

Tripwire:

http://www.tripwire.com/products/

Whereas this product does not analyze the logs, ***Tripwire*** is a useful intrusion detection tool. ***Tripwire*** provides protection for file systems. ***Tripwire***'s software works by taking a picture of critical files and sounding the alert when the files change. The changing of the files is the clue that warns the system that possible intrusion is taking place.

Summary:

A thorough understanding of the event log files can assist in maintaining a secure computing environment. Auditing must be configured and enabled in such a way that meaningful information is collected. The event logs should be collected from all networked systems and stored in a central location. The amalgamated logs can then be analyzed to find and detect intrusions.

As Windows NT and Windows 2000 are more fully deployed in environments requiring high security, more advanced tools to analyze the event logs will be developed. As various forms of artificial intelligence are deployed to analyze the event logs, the effectiveness of IDS systems will be improved. Any overall security strategy must incorporate analysis of the Windows NT security log to detect and isolate intrusion attempts which have overcome other security measures including authentication and access control.

References

Account Lockout Event Also Stored in Security Event Log on Domain Controller - Microsoft Knowledge Base Article Q182918
http://support.microsoft.com/support/kb/articles/q182/9/18.asp

Auditing User Authentication - Microsoft Knowledge Base Article Q174073
http://support.microsoft.com/support/kb/articles/q174/0/73.asp

How to Identify the User Who Changed the Administrator Password - Microsoft Knowledge Base Article Q173939
http://support.microsoft.com/support/kb/articles/q173/9/39.asp

Introducing the NT Security Log - Smith, Franklin, Windows 2000 Magazine, March 2000

Interpreting the NT Security Log - Smith, Franklin, Windows 2000 Magazine, April 2000

Microsoft Security Configuration Manager for Windows NT 4 - Microsoft Technote
http://www.microsoft.com/technet/winnt/winntas/technote/scmnt4.asp

Monitoring Privileges and Administrators in the NT Security Log - Smith, Franklin, Windows 2000 Magazine, June2000

Protecting the NT Security Log - Smith, Franklin, Windows 2000 Magazine, July 2000

Real-Time Intrusion Detection for Windows NT Based on Navy IT-21 Audit Policy - Kremer, Steven H, MASc Thesis, San Diego State University, September 1999 - http://www.cs.nps.navy.mil/people/faculty/rowe/kremerthesis.htm

Security Event Descriptions - Microsoft Knowledge Base Article Q174074
http://support.microsoft.com/support/kb/articles/q174/0/74.asp

Windows NT Security: Step by Step - Fossen, Jason, and Jennifer Kolde, The SANS Institute GIAC Training, 2000.