Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

An In-Dept Examination of Event Viewer and Auditing

Ruth Parish
November 12, 2000

Information security, systems' security, Internet security, the list goes on and on. A System Administrator's task is becoming more difficult every year, if not every day. Moore's law states that computational speed doubles every 18 months, but it seems that law has been broken of late. A domain or system audit can be developed from a wide variety of commands and utilities. These commands and utilities come from a extensive list of sources including: the hacker/cracker community, shareware, 3rd party vendors, and Microsoft. There are such a great number of settings, i.e.: ports, activities, users, hardware and software to audit, that it is easy for the System Administrator to give up before even beginning.

Almost every article and book that covers security discusses the Event Viewer and auditing. That is to say they cover them *briefly*. They usually indicate that security auditing is turned on in "User Manager," and viewed through the "Event Viewer," and some even go so far to tell you which type of events should be monitored, but they usually stop there. In my small domain we recorded over 28,000 security events in 4 days! Most system administrators take one look at the number of events and throw up their hands. "How," we say, "are we supposed to be able to interpret that amount of data?" What the books don't cover is how to how to collect the data, how to organize and how to interpret the data. And most of all, they don't explain how to do this automatically so it doesn't consume your entire workday, every day. Now don't get too excited, I won't be able to cover all that ground in this short article either. I am convinced that an entire book can be written on Windows NT Auditing and interpreting the Event Viewer alone. What this article will try to do is help you start out with enough information on this subject to do your system administration job succinctly without cutting any corners.

Theory

Whenever I teach, I initially ask the students to put down their pencils for a few minutes and abstain from taking any notes. I tell them that before we get down to the particular commands, etceteras, it is important to understand the theory behind the process.

First, security auditing is controlled and turned on through "User Manager," with file and directory auditing accessible through Microsoft Windows Explorer. The events are recorded and viewed through the "Event Viewer," which displays many additional events from the system and many types of applications. Because of the vast quantity of data and the limitations of Event Viewer it is far more useful to export the data to a database such as Microsoft Access. The Event Viewer logs can be exported via a Microsoft Resource utility called "DumpEL." Since you will want to export the data on a daily or weekly basis, the export process can be automated from a standard Microsoft scheduler program called "AT." That's the short version, here it is again, with each of the major steps listed:

Auditing Milestones
1. Turn on security auditing in "User Manager for Domains."
2. Turn on file and directory auditing through Microsoft Windows Explorer.
3. Export the data with DumpEL.
4. Import the data into a database.
5. Analyze the data.

The Software

Event Viewer – the Basics

"Your overall security strategy depends on the Windows NT security log, which is your final layer of defense for catching violators who made it past your previous layers of authentication and access control." This is a quote from a Microsoft TechNet article on Event Viewer. As an aside, if you are not familiar with TechNet and manage a domain, either small or large, it is a must-have tool for the System Administrator. Microsoft says "Microsoft TechNet is the most comprehensive source of technical information and resources available, designed to help anyone who deploys, maintains, and supports Microsoft products." Once you sign up for TechNet, at a surprisingly low cost, your will receive 5 or 6 CDs every month with the latest Service Packs, Resource Kits, Option Packs, technical articles and much more. Trying to perform an audit whether one time or ongoing without the massive amount of information available through TechNet is like buying an automobile without the Operator's Manual.

Event Viewer is composed of three separate logs, which can all be examined through the Event Viewer interface. The logs are the System log, the Security log and the Application log. What each log records is self evident: the System log tracks system functions, the Application log tracks application events and the security log tracks security events on users, services, etc. Most events that occur on your Window's NT system will be published here. However, there are some exceptions including Proxy logs.

Lets take a look at one of the logs, in this case the Application log, which will give you the basic look and feel of Event Viewer. A note here, all of the screen captures are from an actual system, so the names have been obliterated, or in some cases changed to protect the system.
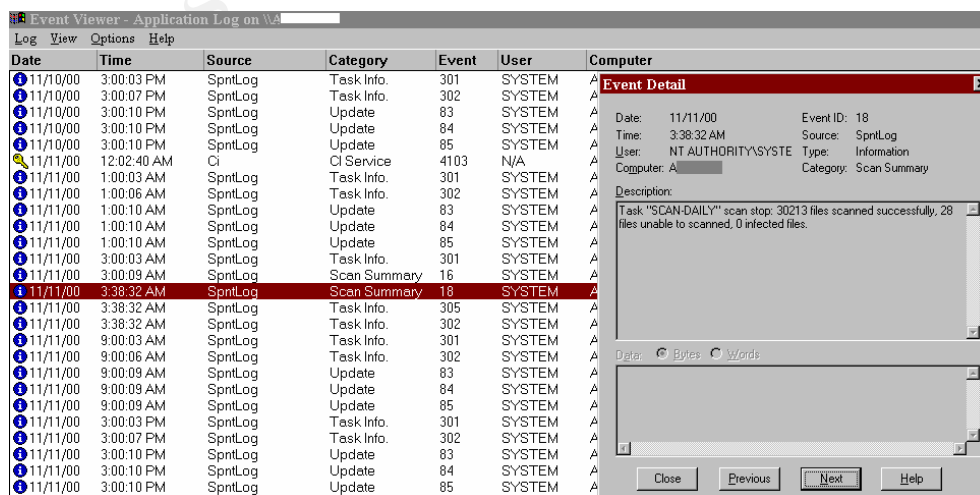
Event Viewer, while limited, does have some useful functionality as shown in these views of the menus.
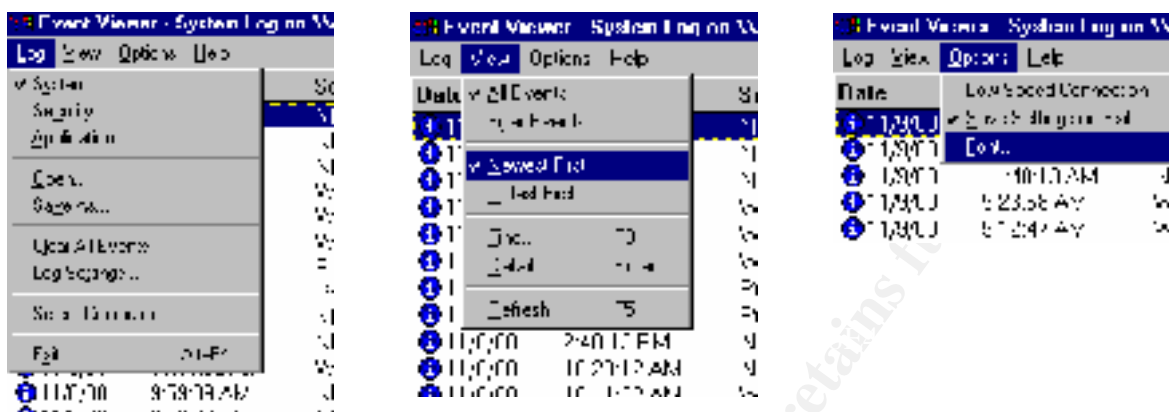
One of the more interesting options to note is the ability to look at a remote computer, by using the "Select Computer" option in the "Log" menu. Another useful option is the "Filter Events" option in the "View" menu.
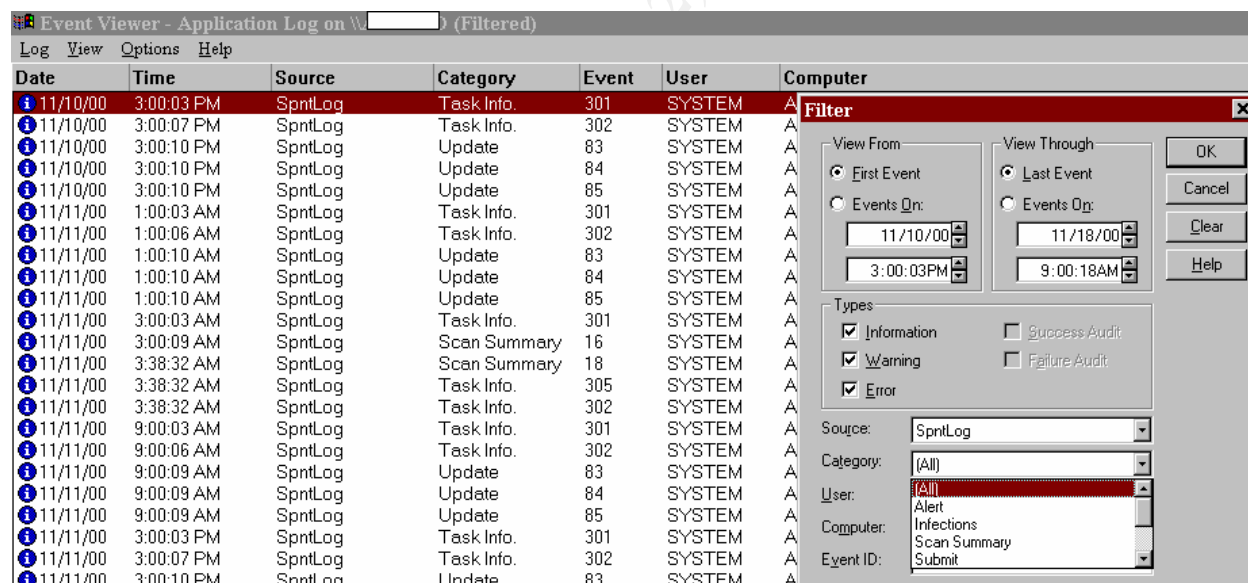
As you can see this is extremely helpful in monitoring specific events in your domain. In the example above the "Source" is the "SpntLog" which is a virus software specifically tasked to protect an NT server. Since this server is locked up and on another floor, it becomes impractical to go there several times a day to check the server. When a new virus hits the network it is very important to keep an eye on the virus situation on all the servers. Note the ability to further filter the data on specific types of 'SpntLog' events, by restricting the type of Category.

Each event can be looked at in more detail, as shown below.
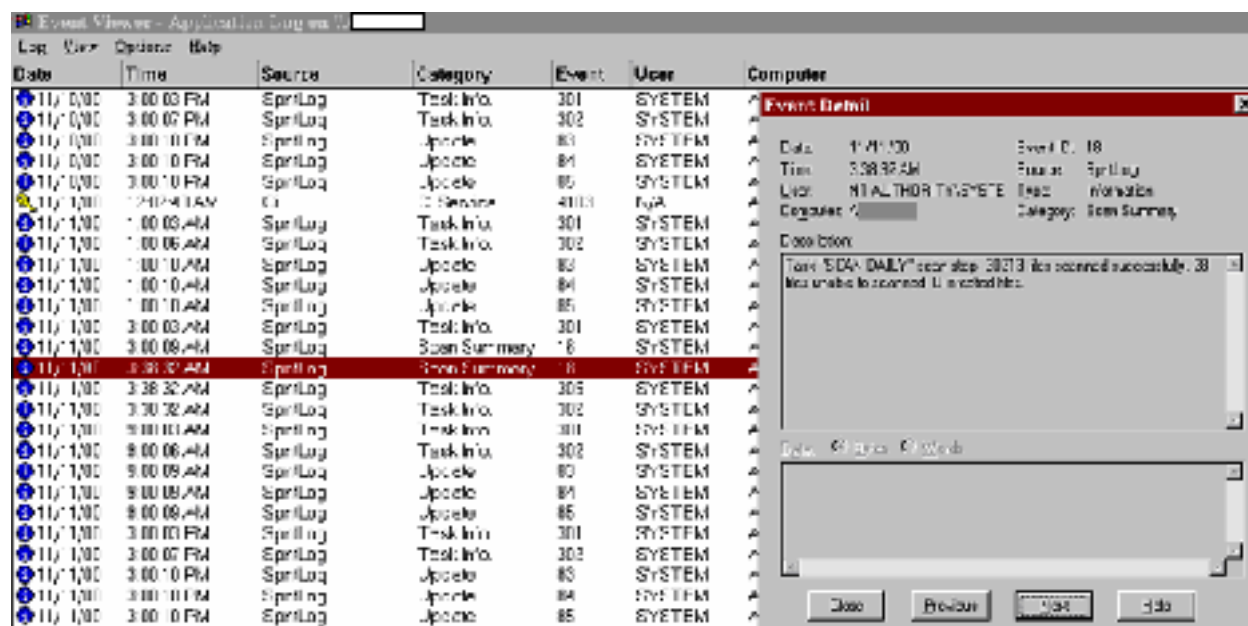
The "Description" can be especially helpful, but occasionally you will be befuddled. Your best resource in these situations is to consult the TechNet CDs, Microsoft Web sites or if you have contract technical support, calling Microsoft or the vendor related to the problem software.

Protecting the Event Viewer and its Data – Best Practices

Expanding on previous SANS articles (see References), the event viewer logs can be viewed by anyone, except the Security log. The security log can only be viewed and cleared by accounts that have been given the "Manage Auditing and Security Log" user right. This right also provides the access to change the system access control lists on files, folders, printers and registry keys.

A note in Jason Fossen's manual, *Securing Windows NT, Step-by-Step* indicates "An earlier bug which allowed Administrators to view/clear the Security Log even if they did not have the SeSecurityPrivilege right has been corrected with Service Pack 4." A must security measure is to ensure that your domain stays abreast of the current Microsoft Service Packs, which often, if not always, contain security patches.

A Microsoft TechNet article, *The NT Security Log – Your Best and Last Defense* suggests to also control guest access to all logs. "… set the Registry key RestrictGuestAccess of type REG_DWORD to HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services /Eventlog*LogName* …"
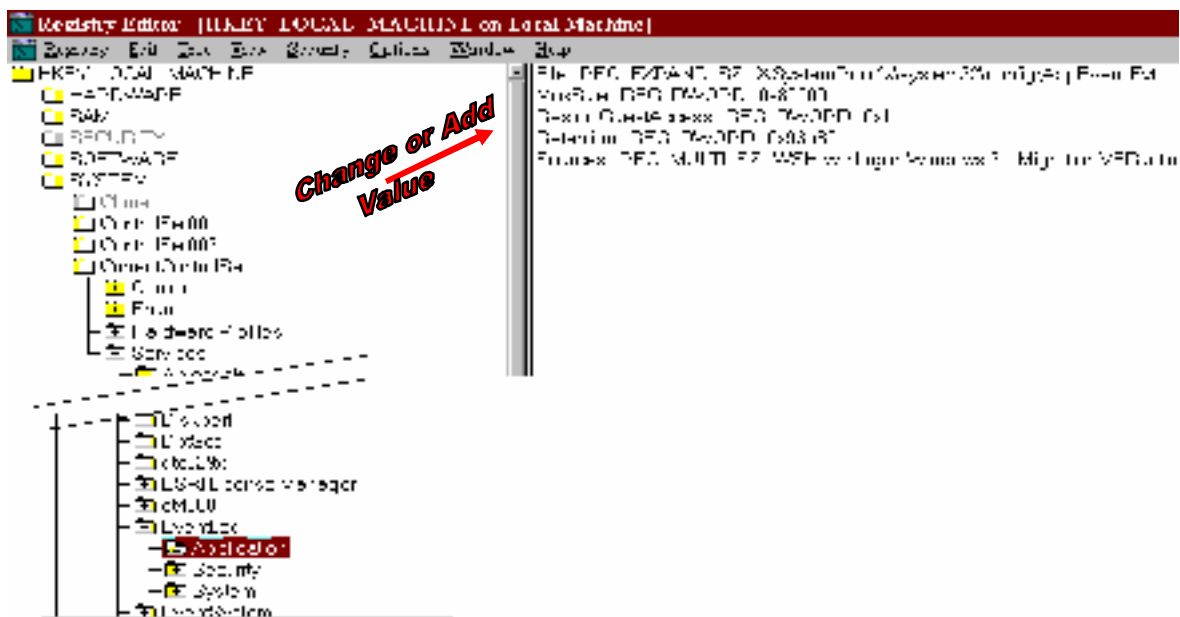
The logs themselves are stored in the "systemroot\system32\config" folder and the file names all end in "…EVENT.EVT." The application log starts with "APP," the security log with "SEC," and the System log with "SYS."

Expanding on previous SANS articles (see References), an experienced hacker will be aware of these logs and attempt to prevent the System Administrator from viewing his/her actions. *Microsoft Windows NT 4.0 Security, Audit, and Control* technical reference manual suggests that "The best way to secure these files is to create an auditor group that has access to these files, and then take it away from all other groups."

Protecting the Event Viewer's Data – Best Practices

There are two property type settings for each log file, its "Maximum Log Size" and how "Event Log Wrapping" will occur. By default each log is original set to 512k in size and will "Overwrite Events Older" than 7 days.
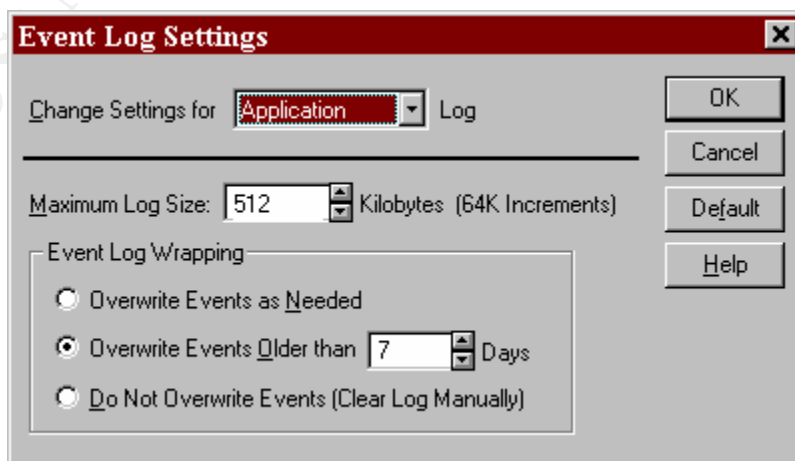
The Microsoft *Windows NT 4.0 Security, Audit, and Control* book states, best, the importance of log file maintenance: "Maintenance of log files is a critical security control that is usually overlooked. Systems administrators take the time to review and implement audit settings. However, a good hacker can create problems that cause the logs to fill quickly and if the proper settings are not set, the logs will overwrite previous log information, essentially erasing the hacker's tracks or crashing the system, causing a denial-of-service attack. Therefore, it is critical that the log parameters for size and event recording for each log are set appropriately."

Expanding on previous SANS articles (see References), size is determined by what applications are running and what type of security auditing is being performed. If you have Microsoft Internet Information Server running, your log files may be quite large, as much as 100MBs (according to Jason Fossen in his manual *Securing Internet Information Server 5.0*) or more. If your server is simply a file server and you are not auditing file and object access, the file might be only a couple of mega-bytes. Unfortunately there is no hard and fast rules, but merely guidelines. You will need to research the special requirements for your particular non-standard applications and add them to the standard guidelines to determine the settings required for each server and workstation. You should then monitor your logs over time to determine that the size setting is correct and serving your auditing needs. Keep in mind that every time you install a new application that the log settings may require new thought. The following are log size suggestions by various authors.

1. SANS security article: *Auditing Windows NT* by Chris Benton. Chris says, "One of the first things I like to do is bump up the maximum size of each of the logs to 8 megs or so. Disk space is cheap…"
2. Microsoft's technical reference manual, *Microsoft Windows NT 4.0 Security, Audit, and Control*, p. 58, suggests the following sizes for specific logs and servers.

Log	Domain Controller	File and Print Server	Database Server	Web Server	RAS Servers	Workstation
Security	5-10mb	2-4mb	2-4mb	2-4mb	5-10mb	1mb
System	1-2mb	1-2mb	1-2mb	1-2mb	1-2mb	1mb
Application	1-2mb	1-2mb	1-2mb	1-2mb	1-2mb	1mb

3. The TechNet article: *The NT Security Log – Your Best and Last Defense* indicates "The amount of log space you consume daily depends on the size and activity of your system; the event categories you enable for auditing in the Start menu's Programs, Administrative Tools, User Manager for Policies, Audit dialog box; and especially the level of object auditing you're using. Therefore, I set the maximum log size to 14mb to accommodate a month of unusually high activity."
4. Jason Fossen's manual *Windows NT Security: Step-by-Step* relates the following information on log file sizes: "From a security standpoint, the System and Application logs are mainly used for analyzing Denial of Service attacks. An exception to this are services which write extensive data to the Application log. … The Security log is the most important and should have a relatively large size and be archived frequently to

prevent its overflow. There are many variables which must be considered when choosing a Security log file size, including:

- Free space on Boot partition.
- Average rate at which the log fills.
- Export/backup schedule for the log.
- Audit policy settings in User Manager.
- Audit options on the SACLs of objects.
- Security policy requirements of one's environment.

These variables must be considered and configured together as a set."

Before the final determination of the size of your log files, you must factor in your Event Viewer "Overwrite" property, as they go hand in hand. Referring back to our sources:

1. SANS security article: *Auditing Windows NT* by Chris Benton. On the overwriting issue, Chris says, "Which setting to use is a judgment call on your part. Obviously from a security perspective the "Do Not Overwrite" setting is best. The only problems is that NT has a really bad habit of crashing when its logs become full. With this in mind you may wish to opt for the "Overwrite as needed setting." If you are using a very large log size, this setting should probably not be a problem. Again, it's a judgment call. Go with the setting that you feel most comfortable with."

2. Microsoft's technical reference manual, *Microsoft Windows NT 4.0 Security, Audit, and Control*, p. 58, suggests "… In our experience, for the Security Log, we have noted that the best practice is to make sure that the size of the log is big enough to hold 14 days of events online." They also suggest the following specific settings for each log.

Log	Overwrite Policy Setting
Security	Overwrite events older than 14 days.
System	Overwrite events older than 14 days.
Application	Overwrite events as necessary.

3. The TechNet article: *The NT Security Log – Your Best and Last Defense* suggests "I also set the event log wrapping to overwrite events older than 3 days because nobody checks the system from Friday evening until early Monday morning. If a process goes awry during the weekend and starts pouring events into the log, NT overwrites older events up to the 3-day threshold and stops logging at that point. By the time I come in Monday, I can at least get a clue as to what happened between Friday evening and Monday morning. .. If I keep a minimum of 30 days of activity online and archive once a month, I can research through 12 months of activity and avoid manually repeating work."

4. Jason Fossen's manual: *Windows NT Security: Step-by-Step* indicates: "The wrapping option to Overwrite Events As Needed should not be used. This option allows an attacker to flush out log files with meaningless entries. … In most environments, the option to Overwrite Events Older Than *X* Days is the best choice. The number of days set should correspond to the log's backup/export schedule. … The option to Do Not Overwrite Events is preferred in very high security environments."

As you can see there are a lot of different opinions here. Here are my suggestions.

1. Export your data daily and import it into a separate database, which you would back up daily, of course.
2. Disk space is cheap, so start out with a good size file, like Chris Benton says, of at least 8MBs. Bump this size to take in vendor advice on your non-standard applications. Make sure you have a big enough disk, don't forget the disk may have a page file; remember to factor in the maximum possible file size.
3. Turn on all of the auditing you will be tracking and then initially set your "Overwrite" setting to "Overwrite as Needed" and see if the 8MB setting was realistic based on your "ideal" length of time you would like to have "live" Event Viewer data. Bump the size until you reach your "ideal" and then add a minimum of a 30% percent margin. Then set your "Overwrite" setting to "Overwrite Events Older than X Days" where X is your retention time.

Note 1: The Microsoft security manual points out that you can force the machine to crash when the audit (security) log is full. Using REGEDT32 set the Registry key:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Control\Lsa
Value Name:	CrashOnAuditFail
Value Data:	1

If it is not set to 0, the system will not crash and the Administrator account will be warned that a particular event log is full. Setting the flag to 1 "is a double-edged sword and should be thought out carefully. Hackers like to generate lots of audit messages, fill the Audit log so that it cannot accept any more messages and then commit malicious acts, which are not logged. If the flag is set, the system will halt when the log is full and the hacker cannot commit any malicious acts. However, setting the flag and halting the system also invokes a denial-of-service attack." The *Windows NT Security: Step-by-Step* manual indicates that "only an administrator will be able to log on" after this kind of system crash because the CrashOnAuditFail has been reset to 2. "The administrator should then archive the Security log, clear the Security log, reset the CrashOnAuditFailt to 1, and reboot."

Note 2: Event Viewer has a nasty trick of not immediately increasing your log space when you indicate a new size. The TechNet article *The NT Security Log – Your Best and Last Defense* relates "After you change the size, you're given the option to save the log. If you don't clear the log, NT won't take advantage of the newly added space."

User Manager – Security Auditing

Security Auditing is the beginning of any good auditing process. James Jumes says in his book "*Auditing* means measuring the system against a predefined system setting to ensure no changes have occurred. Changes may indicate possible security breaches. … These logs support individual accountability by recording user actions. The audit log is also potential evidence for legal or administrative actions. It also services as an assurance tool, revealing how well the security mechanisms are working."

The audit events that are recorded in the Security log are turned on in the "User Manager." The Audit settings are accessed from the "Policies" menu. As you can see in the screen capture below, all auditing is turned off by default. This is fortuitous since logging can, at times, depending on your domain's setup, use up quite a bit of resources and as mentioned before crash the system.

What auditing to turn on is the next question, and everyone seems to have a different opinion. What most sources agree on is that the following group should be turned on for standard auditing.

1. Logon and Logoff
2. User and Group Management
3. Security Policy Change
4. Restart, Shutdown and System

Once auditing is set on a domain controller, it is set on all DCs. Auditing on other types of servers or workstations only audits that machine. In Windows NT Security: Step-by-Step, Jason Fossen warns "Beware of auditing indiscriminately. Excessive auditing can significantly slow system performance. Only audit those rights and objects which will yield *useful* information."

User Manager Auditing – Best Practices

On page 46 of the *Microsoft Windows NT4.0 Security, Audit, and Control* manual it suggests the following audit policy for domains. The table has been broken into 2 tables to enhance readability.

Domain Users' Audit Policy – Domain Controller/RAS Server/File & Print Server

Audit Feature	Description	Domain Controller	RAS Server	File and Print
Logon & Off	Enables auditing of logon/off attempts, and breaking of network connections to servers.	Select Failure	Select Failure	Do Not Select
Use of User Rights	Enables auditing of attempts to user rights that have/have not been granted	Select Failure	Select Failure	Do Not Select
User & Group Management	Enables auditing of creation, deletion, and modification of user and group accounts.	Select Success	Select Success	Do Not Select
Security Policy Changes	Enables auditing of creation, deletion, and modification of user and group accounts.	Select Success & Failure	Select Success & Failure	Do Not Select
File and Object Access	Enables the ability to turn on the auditing of access to a directory or file that is set for auditing.	Select Failure	Select Failure	Select Failure
Restart, Shutdown, and System	Enables auditing of shutdowns and restarts of the computer, the filling of the Audit Log, and the discarding of audit entries if the Audit Log is already full.	Select Success & Failure	Select Success & Failure	Select Success & Failure
Process Tracking	Enables auditing of the starting and stopping processes.	Do Not Select	Do Not Select	Do Not Select

Domain Users' Audit Policy – Database Server/Web Server/Workstation

| Audit Feature	Description	Database	Web Server	Work-Station
Logon & Off	Enables auditing of logon/off attempts, and breaking of network connections to servers.	Select Failure	Do Not Select	Do Not Select
Use of User Rights	Enables auditing of attempts to user rights that have/have not been granted	Do Not Select	Do Not Select	Do Not Select
User & Group Management	Enables auditing of creation, deletion, and modification of user and group accounts.	Do Not Select	Do Not Select	Do Not Select
Security	Enables auditing of creation, deletion,	Do Not	Do Not	Do Not

Policy Changes	and modification of user and group accounts.	Select	Select	Select
File and Object Access	Enables the ability to turn on the auditing of access to a directory or file that is set for auditing.	Select Success & Failure	Do Not Select	Do Not Select
Restart, Shutdown, and System	Enables auditing of shutdowns and restarts of the computer, the filling of the Audit Log, and the discarding of audit entries if the Audit Log is already full.	Select Success & Failure	Select Success & Failure	Do Not Select
Process Tracking	Enables auditing of the starting and stopping processes.	Do Not Select	Do Not Select	Do Not Select

File and Directory Auditing

File and directory auditing can be very useful, but if not used properly can generate a tremendous amount of events. You can audit all users, all resources or just specific users actions or monitor certain critical resources. Don't forget you must enable "File and Object Access" in User Manager Audit Policy for any auditing to be recorded in the Event Viewer.

We had a situation in our company several months ago, where directory and file auditing would have proved very useful. We had a folder where 75% of the sub-folders just disappeared. Unfortunately the problem wasn't noticed for several days. While we were able to immediately restore the data, there was a considerable concern over who deleted the data and why. Did they maliciously destroy the folders or accidentally? Before you can answer that question, you need to know who the *Who* was that deleted the data. Everyone makes mistakes, but the person that deleted that information, if it was accidentally, obviously need retraining and possibly their access needed to be restricted. Without knowing who the culprit was, there is no way to prevent future occurrences.

Setting up directory or file auditing is accessed through "Auditing" button in the file or directory "Properties" window.
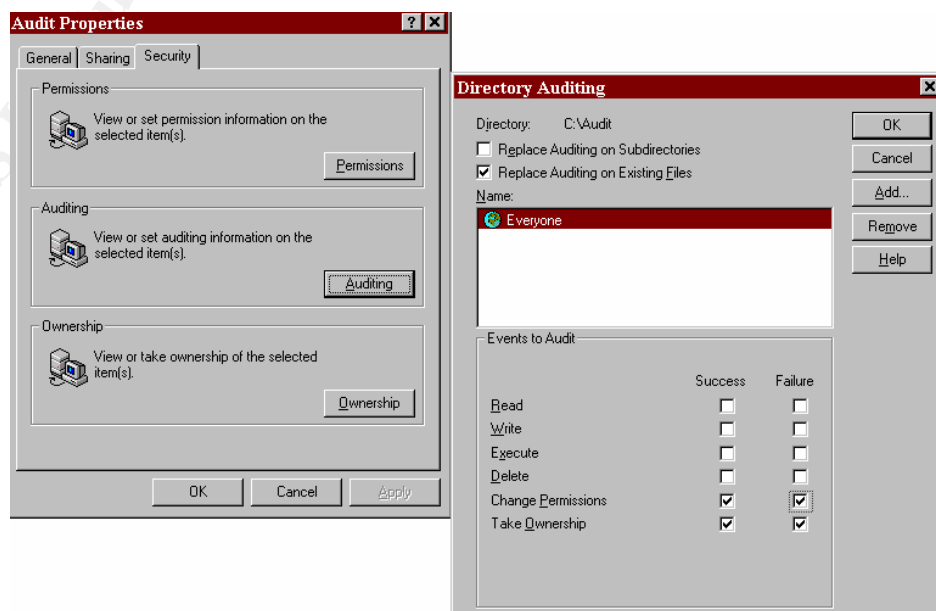
File and Directory Auditing – Best Practices

Microsoft Windows NT 4.0 Security, Audit, and Control technical reference manual suggest the following file and directory audit policies for domain data files.

Item	Success	Failure
Read	Do Not Select	Select
Write	Do Not Select	Do Not Select
Execute	Do Not Select	Do Not Select
Delete	Select	Select
Change Permissions	Select	Select
Take Ownership	Select	Select

Auditing a Special File – The Registry

Don't forget to audit the most important data on your system, the Registry. James Jumes says "Noting any changes that take place in the Registry is crucial for maintaining the integrity, confidentiality, and availability of your systems. … If someone manages to gain physical access to a domain controller or if there are many administrators in a corporation, it is highly recommended to implement Registry auditing as a security control to determine who made the modifications."

Access the auditing feature through the REGEDT32.EXE utility from the "Run" command.
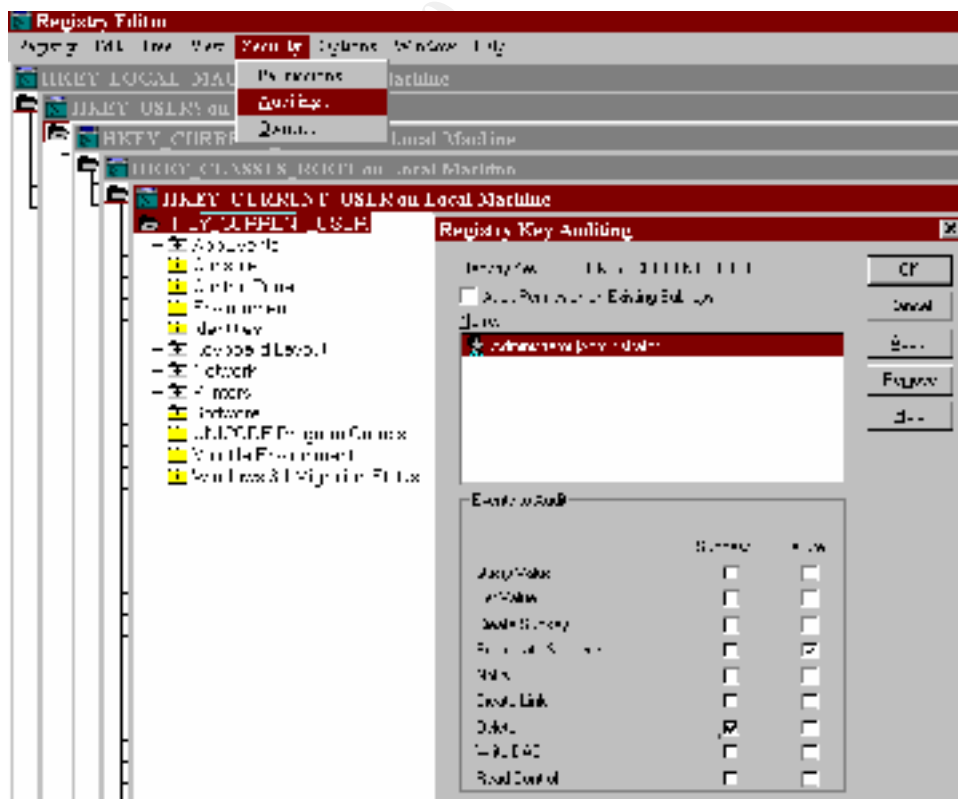
Registry Auditing – Best Practices

Microsoft Windows NT 4.0 Security, Audit, and Control recommends auditing these three keys and their subkeys and the settings shown in the table below.

- HKEY_LOCAL_MACHINE\System
- HKEY_LOCAL_MACHINE\Software
- HKEY_CLASSES_ROOT

Recommended Registry Auditing Options

Item	Recommendation
Query Value	Do Not Select
Set Value	Select Success and Failure
Create Subkey	Select Success and Failure
Enumerate Subkeys	Do Not Select
Notify	Do Not Select
Create Link	Select Success and Failure
Delete	Select Success and Failure
Write DAC	Select Success and Failure
Read Control	Do Not Select

Writing Custom Events to the Event Viewer

You can design and write "custom" events to the event viewer. This can be a very useful tool enabling you to track events and explanation of events. As an example you can log explanations to the log whenever you have a planned shutdown.

Logging events is done through the Microsoft Resource Kit utility LOGEVENT.EXE. It has 3 switches: -M = Log event on specified computer, -S = Log with the specified severity, and –C log event with the specified category. The severity values are: S = Success audit, F = Failure Audit, I = Information event, W = Warning Event, E = Error Event. Categories are shown as numbers. For more information on Categories, see the section the DUMPEL.EXE utility.

Usage can be obtained in the normal way:
LOGEVENT /?

The standard usage is:
LOGEVERNT [-M \\computer] -[S severity] [-C category] text

The usage showing the example above:
LOGEVENT –M \\ThePDC -S I "Weekly restart."

Moving the Data

Now that you have set up auditing and have thousands of events being recorded on numerous machines, how do you manage all of it? All of the best methodologies suggest that you export all of your Event Viewer data from all the servers into a database such as Access or SQL. In Jason Fossen book he covers several types of export utilities: Microsoft's DUMPEL.EXE, SomarSoft's DUMPEVT.EXT, Adiscon's EVNTSLOG.EXE & NTSLOG which will move the data to a UNIX Syslog daemon, BindView's NOSadmin, SystemTools.COM's ELM and Aelita's EventAdmin. All of these utilities have different strengths and of course, different prices.

Moving the Data – Through the DUMPEL Utility

DUMPEL.EXE is a Microsoft Resource Kit Utility. Basically the utility takes much of the Event Viewer data and outputs it to a text file. You can specify the format, what computer it comes from, where the text file is to be placed and the text file type. The following screen capture is a description of its usage.
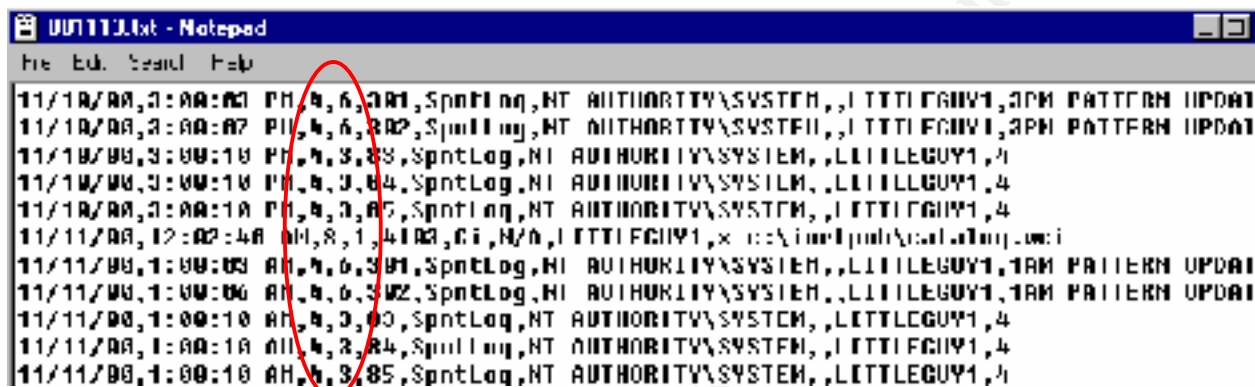
The following example shows that the application event log of the current computer has been output using commas as the delimiters between fields.

```
C:\>dumpel -f c:\reviewer\application\001113.txt -l application -c
Dump successfully completed.
```

And here is an example of the DUMPEL output.

```
001113.txt - Notepad

File  Edit  Search  Help

11/10/00,3:00:03 PM,4,6,301,SpntLog,NT AUTHORITY\SYSTEM,,LITTLEGUY1,3PM PATTERN UPDAT
11/10/00,3:00:07 PM,4,6,302,SpntLog,NT AUTHORITY\SYSTEM,,LITTLEGUY1,3PM PATTERN UPDAT
11/10/00,3:00:10 PM,4,3,83,SpntLog,NT AUTHORITY\SYSTEM,,LITTLEGUY1,4
11/10/00,3:00:10 PM,4,3,84,SpntLog,NT AUTHORITY\SYSTEM,,LITTLEGUY1,4
11/10/00,3:00:10 PM,4,3,85,SpntLog,NT AUTHORITY\SYSTEM,,LITTLEGUY1,4
11/11/00,12:02:48 AM,8,1,4102,Ci,N/A,LITTLEGUY1,x c:\inetpub\scalatmp.wci
11/11/00,1:00:03 AM,4,6,301,SpntLog,NT AUTHORITY\SYSTEM,,LITTLEGUY1,1AM PATTERN UPDAT
11/11/00,1:00:06 AM,4,6,302,SpntLog,NT AUTHORITY\SYSTEM,,LITTLEGUY1,1AM PATTERN UPDAT
11/11/00,1:00:10 AM,4,3,83,SpntLog,NT AUTHORITY\SYSTEM,,LITTLEGUY1,4
11/11/00,1:00:10 AM,4,3,84,SpntLog,NT AUTHORITY\SYSTEM,,LITTLEGUY1,4
11/11/00,1:00:10 AM,4,3,85,SpntLog,NT AUTHORITY\SYSTEM,,LITTLEGUY1,4
```

You will notice that the two columns in the output have been changed from strings to numeric variables. These are the Type and Category columns and appear to change depending on the source. They can be correlated in the Event Viewer by filtering for each type of "Source" and then looking at the filter order for "Types" and "Category." It can be painstaking having to do this for each "Source" but very useful.

Expanding on previous SANS articles (see References), not all of the description for each Event ID is output with DUMPEL, but a Microsoft TechNet article shown below lists the ones for standard Microsoft software. Your non-Microsoft vendors can provide this data for your specialty applications.

TechNET Article: Q174074
TITLE: Security Event Descriptions
PRODUCT NAME: Microsoft Windows NT

Event ID	Type	Description &/or Reason
512	Success Audit	Description: Windows NT is starting up.
513	Success Audit	Description: Windows NT is shutting down. All logon sessions will be terminated by this shutdown.
514	Success Audit	Description: An authentication package has been loaded by the Local Security Authority. This authentication package will be used to authenticate logon attempts.
515	Success Audit	Description: A trusted logon process has registered with the Local Security Authority. This logon process will be trusted to submit logon requests.
516	Success Audit	Description: Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss

		of some audits.
517	Success Audit	Description: The audit log was cleared.
518	Success Audit	Description: A notification package has been loaded by the Security Account Manager. This package will be notified of any account or password changes.
528	Success Audit	Description: Successful Logon
529	Failure Audit	Description: Logon Failure Reason: Unknown user name or bad password.
530	Failure Audit	Description: Logon Failure Reason: Account logon time restriction violation.
531	Failure Audit	Description: Logon Failure Reason: Account currently disabled.
532	Failure Audit	Description: Logon Failure Reason: The specified user account has expired.
533	Failure Audit	Description: Logon Failure Reason: User not allowed to logon at this computer.
534	Failure Audit	Description: Logon Failure Reason: The user has not been granted the requested logon.
535	Failure Audit	Description: Logon Failure Reason: The specified account's password has expired.
536	Failure Audit	Description: Logon Failure Reason: The NetLogon component is not active.
537	Failure Audit	Description: Logon Failure Reason: An unexpected error occurred during logon.
538	Success Audit	Description: User Logoff
539	Failure Audit	Description: Logon Failure Reason: Account locked out.
560	Success Audit	Description: Object Open
561	Success Audit	Description: Handle Allocated
562	Success Audit	Description: Handle Closed
563	Success Audit	Description: Object Open for Delete
564	Success Audit	Description: Object Deleted
576	Success Audit	Description: Special privileges assigned to new logon.
577	Success Audit	Description: Privileged Service Called
578	Success Audit	Description: Privileged object operation.
592	Success Audit	Description: A new process has been created.
593	Success Audit	Description: A process has exited.
594	Success Audit	Description: A handle to an object has been duplicated.
595	Success Audit	Description: Indirect access to an object has been obtained.
608	Success Audit	Description: User Right Assigned
609	Success Audit	Description: User Right Removed
610	Success Audit	Description: New Trusted Domain
611	Success Audit	Description: Removing Trusted Domain
612	Success Audit	Description: Audit Policy Change

624	Success Audit	Description: User Account Created
625	Success Audit	Description: User Account Type Change
626	Success Audit	Description: User Account Enabled
627	Success Audit	Description: Change Password Attempt
628	Success Audit	Description: User Account password set
629	Success Audit	Description: User Account Disabled
630	Success Audit	Description: User Account Deleted
631	Success Audit	Description: Global Group Created
632	Success Audit	Description: Global Group Member Added
633	Success Audit	Description: Global Group Member Removed
634	Success Audit	Description: Global Group Deleted
635	Success Audit	Description: Local Group Created
636	Success Audit	Description: Local Group Member Added
637	Success Audit	Description: Local Group Member Removed
638	Success Audit	Description: Local Group Deleted
639	Success Audit	Description: Local Group Changed
640	Success Audit	Description: General Account Database Change
641	Success Audit	Description: Global Group Changed
642	Success Audit	Description: User Account Changed
643	Success Audit	Description: Domain Policy Changed

Moving the Data – DUMPEL Automated – the Batch File

On our system we output all of our logs each day to a central site, where they are then collected and input into Microsoft Access. Here is a sample output file that is automated through the Microsoft scheduler utility called AT.

```
rem Copy event viewer data to daily file.
rem Standard output for all 3 event viewer logs.

dumpel -l system -s PDCputer -t -format dtTCISucs >
      c:\ev\system\%AuDATE%.txt
dumpel -l application -s PDCputer -t -format dtTCISucs >
      c:\ev\application\%AuDATE%.txt
dumpel -l security -m security -e 528 529 538 539 -s PDCputer -t -format
      dtTCISucs > c:\ev\logonoff\%AuDATE%.txt

dumpel -l system -s DC1puter -t -format dtTCISucs >
      c:\ev\system\%AuDATE%.txt
dumpel -l application -s DC1puter -t -format dtTCISucs >
      c:\ev\application\%AuDATE%.txt
```

```
        dumpel -l system -s DC2puter -t -format dtTCISucs >
             c:\ev\system\%AuDATE%.txt
        dumpel -l application -s DC2puter -t -format dtTCISucs >
             c:\ev\application\%AuDATE%.txt

        dumpel -l system -s MEM1puter -t -format dtTCISucs >
             c:\ev\system\%AuDATE%.txt
        dumpel -l application -s MEM1puter -t -format dtTCISucs >
             c:\ev\application\%AuDATE%.txt
```
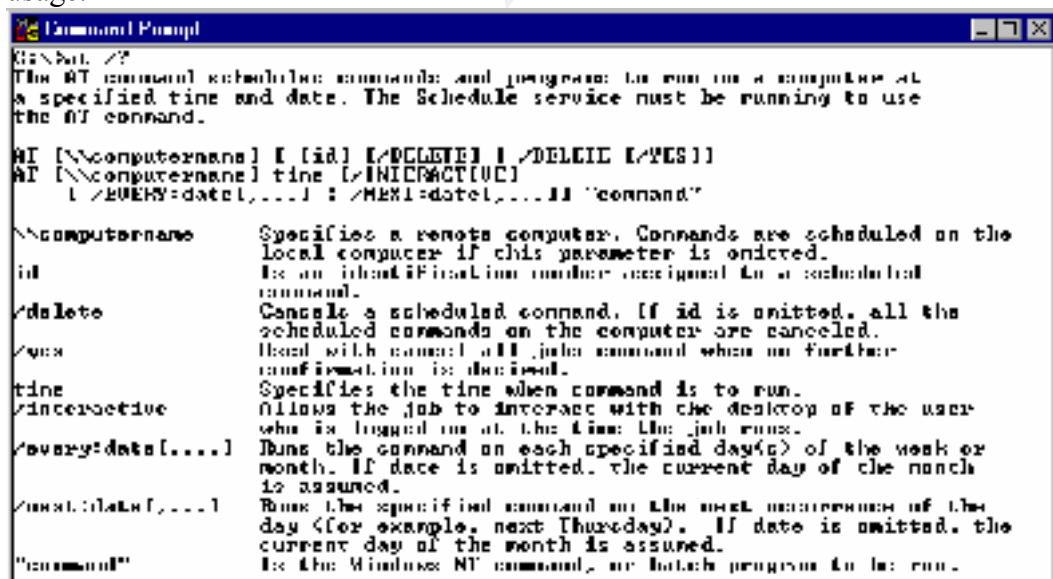
You will note, in the first group for PDCputer, ("puter" is slang for computer) that a very specific set of event IDs is output to its own separate text file. These IDs are the events that show successful and failed domain logoffs and logons. Also note that the batch file outputs the Event Viewer data with the tab delimiter. Many of the string values in Event Viewer have embedded commas, so the standard output format becomes spread across several fields.

There is a similar batch file run on each of the domain controllers that outputs its individual security file and one showing logons and offs.

Moving the Data – DUMPEL Automated – Scheduling

The Microsoft NT scheduler utility AT is essential to any system administrator. There is also a windows GUI version called WINAT in the Microsoft Resource kit. The following shows its usage.

Note that you can submit a batch job on another server or workstation, assuming you have the right.

Here are a couple of examples.

Adding a job:

```
C:\>at 00:01 /every:m,t,w,th,f,s,su e:\eu\output.bat
Added a new job with job ID = 5

C:\>at
Status ID   Day                     Time            Command Line
-------------------------------------------------------------------------------
        0   Each Su                 4:30 AM         c:\reboot\shutdown /L /Y /R /C

        1   Each M T W Th F S Su     12:01 AM        c:\eu\output.bat
        5   Each M T W Th F S Su     12:01 AM        c:\eu\output.bat
```

Deleting a Job

```
C:\>at
Status ID   Day                     Time            Command Line
-------------------------------------------------------------------------------
        0   Each Su                 4:30 AM         c:\reboot\shutdown /L /Y /R /C

        1   Each M T W Th F S Su     12:01 AM        c:\eu\output.bat
        5   Each M T W Th F S Su     12:01 AM        c:\eu\output.bat

C:\>at 5 /delete

C:\>at
Status ID   Day                     Time            Command Line
-------------------------------------------------------------------------------
        0   Each Su                 4:30 AM         c:\reboot\shutdown /L /Y /R /C

        1   Each M T W Th F S Su     12:01 AM        c:\eu\output.bat
```

Organizing Your Event Viewer Data in a Database

We maintain an Access database with all of our Event Viewer data from servers throughout the domain. This enables us to correlate related material from different machines and different time periods.

Each event log type, application, system, and security are exported and then input into its own individual table. Queries and reports have been developed to show specific types of information that we wish to monitor.

Date	Time	ID	Domain User	Computer	User	Type	Process	Authentication
11/10/2000	11:41:15 AM	538	C	A	I	3		
11/10/2000	11:44:35 AM	528	C	A	E	3	KSecDD	MICROSOFT_AUTHEN
11/10/2000	11:47:57 AM	538	C	A	E	3		
11/10/2000	12:17:31 PM	528	C	A	I	3	IIS	MICROSOFT_AUTHEN
11/10/2000	12:41:15 PM	538	C	A	I	3		
11/10/2000	12:44:53 PM	528	C	A	E	3	KSecDD	MICROSOFT_AUTHEN
11/10/2000	12:47:57 PM	538	C	A	E	3		
11/10/2000	1:03:13 PM	528	C	A	I	3	IIS	MICROSOFT_AUTHEN
11/10/2000	1:26:15 PM	538	C	A	I	3		
11/10/2000	1:27:22 PM	528	C	A	I	3	IIS	MICROSOFT_AUTHEN

Above is a view of our Logons table which shows both successful and failed logon and logoff attempts. The type numbers were correlated by Chris Brenton in his SANS article *Auditing Windows NT*.

Type	Description
1	None provided.
2	Interactive logon/logoff.
3	Network logon/logoff.
4	Started by batch process.
5	Started by running service.
6	Proxy Logon.
7	Unlock Console (screen saver).

Data can be viewed in many different types of formats and reports by extensive, but simplistic queries and reports. In this query, the Event ID field is filtered to show all Event IDs below 528 and above 538, but not Event ID 576.

We take tables of Event ID, Type and Category descriptions and add them as separate tables to our database which are then linked to the event tables, where appropriate. This report is an example of culling data to show important information. Note how the Event ID description table has been linked to Event ID numeric field in this report.

ID	Source
Main Table - Security	Main Ta
☑	
<528 Or >538 And Not 576	

Security Event Log Summary by Computer by Day

Description   Computer

Sunday, November 12, 2000

Monday, November 13, 2000

Database – Best Practices

1) Select a database software that your staff is extensively familiar with its abilities. The "best" software is not always the most used, if the staff is unfamiliar with it.
2) Format the database tables enabling daily or weekly event viewer data to be imported as simply and quickly as possible. If this function becomes difficult, the entire auditing may break down. Ideally write code that would automate the data import process.
3) Create queries and reports that reflect your office's audit and security policy requirements.
4) Create queries and reports that help spot hacker activity.
    a) Look for items that shouldn't happen.
    b) Look for activity that shouldn't happen at certain times.
    c) Watch for application activity that should or should not be occurring.
    d) Determine baseline activity, such as how many logons/offs, or shutdowns or certain files should be accessed on a daily and weekly basis.
    e) Use the baseline information for weekly comparisons to highlight standard activity happening at heightened levels. For instance, it is normal to see a certain number of logon failures, but to seem a group start to cluster around one time period or one station would be unusual. You may have an internal user starting to get cute and try to guess or hack into other accounts.
5) Train other administrators on the database procedures, importing data, looking at certain reports, etc.
6) Don't forget the obvious, set SACLs to protect the database, make sure it is backed up as required.
7) Keep generational archives on tape or CD. These can be useful if your security database is ever compromised. It will also provide justification data for future upgrades.

Summary – Best Practices

1) Set up Event Viewer for logging on all Servers.
    a) Determine and set the appropriate size and wrapping settings.
    b) Clear the logs.
    c) *Secure* the Event Viewer logs.
2) Determine and set the appropriate audit policies for your company and domain(s) in "User Manager."
3) Determine and set the appropriate file and directory auditing.
    a) Don't forget to enable "File and Object Access" in User Manager audit policies.
4) Determine and set the appropriate Registry auditing.
5) Set up automated exporting of Event Viewer data.
    a) Create batch files.
    b) Automate batch files with AT.
    c) *Secure your batch files.*
6) Create and set up database for Event Viewer data.
    a) Set up tables.
        i) automate import process.
    b) Create appropriate queries and reports to reflect your companies security policy.
7) *Secure* your database.

8) Document the entire audit plan.
9) Train the Administrator staff on the *plan*. Make sure they can run it when you are sick, on vacation, or run off for that new high-paying job.

Windows NT Auditing is a challenging process to design and implement. Repeating Franklin Smith's statement in his TechNet article, *The NT Security Log – Your Best and Last Defense*. He said "Your overall security strategy depends on the Windows NT security log, which is your final layer of defense for catching violators who made it past your previous layers of authentication and access control." He finishes with "This audit trail lets you detect suspicious activity from both outsiders and insiders and provides you with important evidence to use against intruders."

It is unfortunate that NT auditing is so tedious, but and this is a big but, it is well worth the effort and trouble. Don't be one of the many system administrators that ignore this powerful and illuminating tool. What you don't know can hurt you!

References:

Jumes, James G., et. al. *Microsoft Windows NT 4.0 Security, Audit, and Control.* Redmond Washington: The Microsoft Press, 1999.

Brenton, Chris. *Auditing Windows NT*. Version 1.1. SANS Institute Basic Windows NT Auditing – SANS' Level One 2000.

Automating Detection of Logon Failures in a Windows NT Domain. 1993-2000 Microsoft Corporation. Microsoft Knowledge Base Article ID: Q171148.

Security Event Descriptions. 1993-2000 Microsoft Corporation. Microsoft Knowledge Base Article ID: Q174074.

McDowall, Tracey. *Developments in Auditing NT, Information Technology*. The SANS Institute. (14 November 2000).

Golias, Martin A.. *Practical T1 Track Parliament Hill, Ottawa*. The SANS Institute. (14 November 2000).

Chapter 9 – Monitoring Events. 2000 Microsoft Corporation. Updated: 12 January 2000. URL: http://www.microsoft.com/TechNet/winnt/Winntas/manuals/concept/xcp09.asp (13 November 2000).

Hill, Tim. *Windows NT Shell Scripting*. MacMillian Technical Publishing, 1998.

Smith, Franklin R. *The NT Security Log – Your Best and Last Defense*. 2000 Microsoft Corporation. Updated: 3 August 2000. URL: http://www.microsoft.com/TechNet/winnt/ntsecuri.asp (13 November 2000).

Fossen, Jason. *Securing Windows NT, Step-by-Step, Parts 1-3*. Document Version 3.7. The SANS Institute, 24 July 2000.

Fossen, Jason. *Securing Internet Information Server 5.0*. Document Version 2.0. The SANS Institute, 23 July 2000.