Global Information Assurance Certification Paper

WORKING WITH THE NT EVENT LOGS

By Kris Hartley

If properly setup and secured, the event logs in Windows NT are a good source of information and evidence for the security analyst or administrator. Unfortunately, in their native state, the logs are slow and hard to work with when you are trying to get the information you need. This article is about some easier ways to work with the logs, what the information in the logs mean and how to make sure the logs have the information you want to track. The three event logs in NT and Win. 2000 are the System, Application and the Security logs. I deal mainly with the security event log in this article, but the tools and technics can be used on the other logs as well.

The Event Viewer that comes with NT provides a way to look at the logs, but it isn't very convient or efficient for anything more than a quick peek. For a more efficient and comprehensive look at the event log, you need to get it into a more user-friendly form. A spreadsheet or database makes analyzing the information much quicker, easier and let's you do a more thorough search of your log files. No problem right? Just use the SAVE AS function in event viewer to save the log as a text file and then import it into Excel or Access. Yes, you can do that…..if you only want or need half or less of the information contained in your logs. If you save your event logs this way; you only get the portion of the information that you see in the event viewer window. You don't get the "detailed information" that comes up in the popup window when you double click an event in event viewer.

There are numerous utilities available to get event log data for you and render it into a format that is much easier to work with. DUMPEL, comes with either NT or Win.2000 resource kits. It vastly improves your efficiency at working with event logs. DUMPEVT is a freeware utility available at www.somarsoft.com. DUMPEVT works in a similar fashion to DUMPEL, but in my opinion, DUMPEVT is the better of the two. One reason I prefer DUMPEVT is its ability to only download the incremental differences in the log since you last ran DUMPEVT. That can be a convient feature. Of course, DUMPEVT allows you to dump the entire log by using the /all switch from the command line. It even allows you the option of selecting machine specific, or user specific when retrieving the incremental differences in a log file. That helps eliminate confusion and missed records if two or more people use the same machine to run the utility. Okay, so this is one reason for my preferring DUMPEVT over DUMPEL. Your needs and situation may be different than mine, so I would recommend that you take a look at both and decide which suites you better. The main thing these utilities do is to give you a way to easily work with your log data. I keep a DUMPEVT formatted copy of the security event log from our PDC in text form. Then depending on what I am looking for, I can load info into either EXCEL or ACCESS and work with the data MUCH more efficiently than by using event viewer.

Once you have used a utility to dump your security log and you have it loaded in a database or spreadsheet, now it's time to begin to decipher the often cryptic information that is in a log file. If you aren't already familiar with the meaning of the codes in the column called EVENT ID, and probably even if you are familiar with them, get a copy of what those ID's or codes mean. A list is available at Microsoft's web site. Going to their site and doing a search for "security event descriptions" should get you what you need. When you find it, print it out. Keeping the hard copy handy will be a good idea. There are

a lot of codes and who has time to memorize all of them?

Now that you have your log in an easy to read and search form and you are armed with a list of the meanings of the event ID's, pick out a couple of the ID's and check to see what information for that ID is available in your log file. You'll quickly see that the information you have, and how it is listed, varies from one event ID to another. For example, it's fairly easy to see that an event ID of 528 means a person has logged on, and what their user name is. It can be more challenging to decipher a "642" to see just what was done and who did it. A good way to learn more about exactly what to look for when you are trying to decipher information in an event log, is to get permission to make modifications to a test account. Make changes to that account and then look at the logs to see the modifications you made. Better yet, is to get permission to create an account, then modify it, and again, view the log files for your work. Seeing you're own user name and other information in an event record makes it easier to recognize what information should be where. It can be confusing to look at all of the information listed in the logs for just one event and see, in different columns, something like this: User Name 1FLA\Br00122, LOGIN ID: (0x0 0x6EA33F) and USER ID S-1-5-21-201080092-1077973705-632796215-6080. Assuming for a minute, that all of these "ID's", were in one event log record for a test account that you had been working with, seeing all of these "ID's" can be confusing. The first one, 1FLA\BR00122, probably wouldn't be hard to recognize, since it would just be your DOMAIN then a \ and your USERNAME. The second one, (0x0 0x6EA33F), may mean nothing to you. You know this isn't your ID, so whose is it?
Again, assuming you are looking at a record in the event log that you were working on…..it is your ID. ID's represented in this format are called "session ID's" or "access ID's". They are a unique identifier of a logon session. Each time you logon, you get an ID in that fashion, assigned to your session. It remains until that session is logged off.
The other ID in our example is a SID, or security identifier. They won't be exactly like this one of course, but all SIDs are similar to, or in a format like this S-1-5-21-201080092-1077973705-632796215-6080. A complete discussion of SIDs would be as lengthy as the ID it's self would suggest. When working with event logs, I act as if a SID were only a unique representation of the user account, only in a different format. There is much more to SIDs than that of course, but for our purposes here, that description should work well. If you need to know the SID for a certain user account, there is a Microsoft utility called getsid,exe that will give you that information from the command line. The format for using getsid is, getsid.exe \\servername accountname \\servername accountname. I use the PDC and BDC as my two server choices for this.

When you're working with your event log dump file, you may notice that some common events are not showing up in your file. What events appear in your logs depends on auditing policy settings. Within User Manager, there is a list of categories and for each of those categories, you can choose to audit nothing, successes, failures, or both successes and failures. It could be that your company's audit policy doesn't include some events, or that the auditing policy settings aren't set to meet company standards. In User Manager, the seven categories that can be audited for successes and failures are: Logon and Logoff, File and object access, Use of user rights, User and group management, Security policy changes, Restart & shutdown system, and Process tracking. Find out what your company's auditing policy is, and check on a regular basis to see it is being met. You can check the policy for each server with User Manager or a command line utility

called auditpol.exe. Auditpol comes with later versions of the NT resource kit or with Win. 2000. Remember that you can't get information from the logs for an event that isn't being audited.

Security event logs can provide the information to answer all sort of questions and solve many problems. Once you use a utility like DUMPEL or DUMPEVT to make a copy of your logs that is in a more efficient form, databases, spreadsheets and command line utilities can help you get the most from your logs. I often run the FINDSTR command on a text version of my logs and send the output to a new, smaller file. If, for example, I only need info for a one day time period, within a 100 meg log file, I do a FINDSTR on the date I need and send the output to a new file. That gives me the info I need to work with, but in a file size that' s easily loaded into Excel for further searching or filtering. DUMPEL and DUMPEVT can also bet set to run on scheduled days and times using the AT command. By using the At and the SOON command, you can set them to run automatically more than once a day. At the company I work for now, we had a need to have a list of account names and the date they were created. With DUMPEVT in a batch file, we can get our incremental dumps of the security event logs, then filter that for the event "624" (new account created), filter that info to only include the account name and the create date, then append it to our ongoing list of create dates, then send the incremental dump file to append to the master event dump file. All scheduled, all unattended. A nice, easy, inexpensive solution.

I hope what I've had to say helps you with your event log work. NT's event logging isn't perfect, but it can go a long way toward providing the auditing that's needed in a network environment today. I would like to add that keeping a copy of your logs in their native format is a good practice. Although working with event logs in their native format is slow and tedious; it is generally accepted that for legal evidence, the logs should be available in their native form.

"Security Event Descriptions" Microsoft url:
http://support.microsoft.com/support/kb/articles/Q174/0/74.asp (12/11/00)

"Security Identifiers" Microsoft url:
http://msdn.microsoft.com/library/psdk/winbase/accctrl_38yn.htm (12/11/00)

Smith, Randy Franklin "Interpreting the NT Security Log" url:
http://www.win2000mag.com/Articles/Print.cfm?ArticleID=8288 (12/11/00)

"The Windows NT Security Model" Security on Windows NT, Microsoft url:
http://noyau.com/reference/serk/scwin_1.htm (12/10/00)

Murray, James D. "Windows Event Logging" Sept.98 published by O'Reilly
Description, index, contents and sample chapter available at url:
http://www.oreilly.com/catalog/winlog/ (12/12/00)