Global Information Assurance Certification Paper

Windows 2000 Security Auditing

By,
Hans Yeazel

Submitted 10/19/2003

Abstract:
It is necessary to take control of illegal systems access and identify intruders. Auditing features in Windows 2000 allows system administrators to monitor illegal systems activity either by internal users or external intruders. Aelita InTrust Software has also provided an alternative solution for tracking and logging security violations. You can find more information about Aelita by visiting their website at www.aelita.com.

It is important to first ensure that your Windows 2000 network is in compliance with the necessary requirements to enable auditing features. After identifying that your network is in compliance, you can explore the auditing options that are available to you. Below I will guide you through the steps of ensuring your network is capable of enabling Windows 2000 auditing features, choosing what activity to audit, setting guidelines and policies for auditing and offer you an automated alternative to logging and tracking security violations.

The Necessity of Security Audits:
In today's networking environment, where companies and consumers depend on the privacy and security of their data, it is extremely important to be aware of who is accessing information on your network. Failure to identify intruders can result in malicious activity on your network, mining of private information or data, or even cause your servers and end-user computers to become unstable or non-operational. There have been many situations where people have used their computers and or access with malicious intent such as hacking into networks and stealing data or deploying viruses that can hinder day-to-day business operations.

An important advantage of completing security audits is the ability to detect unauthorized access either to your network or confidential files or folders. By monitoring logon events, a systems administrator is able to identify network logon attempts. These findings allow a company's Security Department the ability to become aware that somebody may be attempting to break in to the company's network. By tracking these logon attempts you are able to piece together a puzzle and identify trends such as what time the intruder was attempting to log onto the network and what files the intruder is attempting to access.

For example, the inability to know who is accessing your networks resources can cause organizations to spend a lot of time and money cleaning up the damage viruses leave behind. A small virus that merely distributes itself throughout a users Microsoft Outlook address book can crash outlook services, which puts a temporary halt on e-mail, a vital communication link for all employees within an organization.

Physical security is also an important item to be audited. Without knowing which employees are leaving hardware exposed and vulnerable to theft, you are able to do nothing about the problem. Spot-check audits should be completed periodically to ensure employees are leaving all hardware and software secured, as well as paper documents. The confidential information that is stolen makes up the largest portion of the cost to an organization when theft occurs, not the cost of the hardware.

How Do I Get Started?

When you come to the realization that security auditing is necessary in your environment, there are several steps you must take to ensure you are able to gather the necessary information to begin your audit tracking. It is necessary that you are certain all steps are covered otherwise you will find that your attempts to track perpetrators are essentially useless.

The first and most critical step to ensure your network is properly configured for security audits is to ensure any FAT16 or FAT 32 drive partitions are converted to NTFS (New Technology File System). NTFS drive partitions are in compliance with the Windows security model. NTFS allows both file and directory permissions to be set on your server. To quickly and easily convert any FAT16 or FAT32 drive partitions to NTFS, follow these directions (Osborne/McGraw-Hill. Windows NT Server 4.0. Berkeley: Brandon A. Nordin, 1998. page 56):

1. Log on to your computer as an administrator
2. Navigate to the Start Menu, then Run
3. In the Run window, type cmd (for command prompt)
4. In the command prompt window, use the conversion utility, *convert.exe*
5. type *C:\Convert D: /FS:NTFS* (This will convert the D partition to NTFS)
6. Once step 5 has been completed, it is necessary to reboot your computer so the file system can convert to NTFS during the boot process.

After you ensure your drive partitions are converted to NTFS, you can now enable your W2000 auditing features. To enable auditing in Windows 2000, you must first ensure the Group Policy snap-in is installed. Now, you are able to identify exactly what you would like to audit. To audit Active Directory (logon attempts, either successful or unsuccessful) follow these directions ("Audit Active Directory Objects in Windows 2000." 6 June, 2003, http://support.microsoft.com/default.aspx?scid=kb;EN-US;q314955):

1. Click on Start, navigate to Programs, navigate to Administrative Tools
2. In the View Menu, click on Advanced Features
3. Right-click on the Domain Controllers container, then click properties
4. Click on the Group Policy tab
5. Click Default Domain Controller Policy, then click on Edit
6. Double-click the following items to open: Computer Configuration, Windows Settings, Security Settings, Local Policies Audit Policy
7. In the right-hand pane, open Audit Directory Services Access
8. Click the options you would like to Audit (Successful Logon Attempts, Unsuccessful Logon Attempts, or both)

In order to enable auditing features on files or folders, follow the instructions listed below ("How to Enable and Apply Security Auditing in Windows 2000." 3 June 2003.

http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q300/5/49.ASP&NoWebContent=1):

1. Click on Start, navigate to Programs, Accessories, then Windows Explorer, then select the file or folder you would like to audit
2. Right-click the file or folder, then click properties
3. Click on the security tab
4. Click on Advanced
5. Click on the Auditing tab
6. To set up auditing for a new group or user:
    a. Click Add. In the name box, type the name of the user you would like to audit.
    b. Click OK to automatically open the Auditing Entry dialog box
7. To view or change auditing for an existing group or user, click the name, then click on View/Edit
8. To Remove auditing for an existing group or user, click the name, then click on Remove
9. Under Access, click Successful, Failed or both Access and Successful, depending on the type of activity you would like to audit.

You have now activated auditing on Active Directory and the files and folders of your choice.

What Activity Can I Audit?

There are several activities that can be audited on your network. Below I will give you a description of each activity that can be audited as well as give you detailed information as to why you would want to audit each activity.

In order to perform audits on logon events or account logon events, described below, you must first ensure that you have Windows 2000 Active Directory Access set up to audit either successful or unsuccessful logon attempts. It may be necessary to enable auditing of all events, successful or unsuccessful, to ensure that you are able to gather as much information as you need to make a detailed analysis of who may be using your network or local resources with malicious intent. If you do not choose to audit unsuccessful logon attempts, you may be missing important information that can lead you to the conclusion that somebody is attempting to access another users account or more importantly that somebody outside your company is attempting to logon to your domain. This critical information can be very helpful in the event that intrusion into your network is detected.

We will begin with auditing account logon events. Auditing account logon events identifies successful account logon events made by a person with an account on your domain. Auditing this activity will allow a systems administrator to see exactly when a user is logging onto the network. For example, say you have a sales department that closes at 5:00pm and you do not want users to logon after that time. Auditing account logon events will allow you to see if indeed somebody is logging in after 5:00pm.

Granted, it is possible to specify a certain timeline for a user to log into the network in W2000 Active Directory, but many companies do not enforce these policies.

Similar to auditing account logon events is auditing logon events. The big difference between the two lies in where the user is logging in. Auditing account logon events audits the logon of a specific user id. This type of audit is appropriate in a shared workstation environment. If users are able to log into a machine of their choice, it is highly recommended that you audit your account logon events. On the other hand, if each user is assigned a workstation and does not have permission to log onto the workstation of their choice, it would be more appropriate to audit logon events.

A different perspective on auditing logon events is that it may be necessary no matter what type of workstation environment you have, shared or not shared. Take for example the scenario that each user in your company has their own workstation, but everybody has permission to sign onto the workstation of their choice. Users in this type of environment may choose to store information on their local hard drives rather than network drives. If it is found that an employee has signed onto a workstation in your environment and used its local resources with malicious intent, it is possible to identify exactly who logged onto that workstation and at what time. This type of auditing is highly recommended due to the fact that some local documents may contain highly confidential information.

Throughout this text I have been and will continue to discuss audit "logs." Generally speaking, these are files that contain your audit information. Administrators can save these logs to a secured network drive if they desire. It is also possible to allow the specific workstation to keep logs of logon events, shut downs and restarts of workstations. To view this information it is necessary to activate the security feature of your systems event log. By navigating to the Start menu, programs, administrative tools, event viewer you have the option to click on the security tab from the logs menu. This view of the event log also gives you the appropriate information needed to audit the events discussed above. Included in the event viewer are the date and time of the event, a description of the event and the user's information. It is important to remember that this information is stored locally on the machine; therefore it is necessary you get the information from the specific machine you are targeting. This would not be an appropriate way to look up logon events by a user id simply because the user could have signed onto any workstation on your network.

Before I go any further, it is important to note that a large part of using secured data with malicious intent comes from company's own employees rather than outside sources. It is critical that systems administrators ensure that employees have access to the resources needed to do their job and no more than that. For example, you would not want a sales associate to have access to payroll records. It is not necessary for the sales associate to have this access to do their job and only tempts that user to access secured and confidential information within those records. Keep this in mind as you read about the numerous auditing activates discussed below.

Auditing account management gives system administrators a more in-depth look at what activity is taking place on a user account. Among the user details that can be audited include addition of a user to a global group and user rights. Global groups are security privileges assigned to a specific user. They are most commonly associated with a secured folder on a shared network drive. Addition of a user to a global group indicates that the user now has permission to access the secured data. Auditing global groups is a highly important part of security for companies in which the systems administrators themselves are not the ones approving or assigning the access. If global groups are not audited thoroughly and frequently you can often overlook the fact that a user has access to a secured resource to which they should not have access. This user is now able to read or edit any of the information shred in that secured folder and can use the information with malicious intent.

An audit of user rights allows a systems administrator to see all access of a specific user account. The rights assigned to a user can indicate what time of the day a user is allowed to log onto the network, their access to shared resources, or even their ability to manipulate settings on their workstation. It is important to audit user rights to ensure employees have access to do their job and their job only. This is often referred to as least privilege access.

Similar to audits of global groups and user rights is auditing object access. Objects are identified as any resource on your network, including files and printers. To audit and object, it must be enabled for the specific object you would like to audit. For example, if you would like to audit access to a shared printer, you would need to enable auditing on that printer. The same is true for a folder on your network drive. If you would like to enable auditing for the "Sales" folder, you would need to enable this functionality on the folder itself. As far as the necessity of auditing object access is concerned, the same holds true as does for auditing of global groups and user rights. You need to make sure that only the proper employees have access to the objects they need to do their job efficiently.

A step above auditing only object access would be process tracking. Process tracking allows systems administrators not only to see when a user accesses an object, such as a file or a printer, but it also allows the administrator to see when a program is activated. For example, if a company closes for the evening and employees return to work the next day to find that their accounting software has been manipulated, it is possible to view your log that holds the process tracking audit for the accounting software. Within the log you would be able to see who came in the office later in the evening and manipulated the data. It would not take long to identify and take corrective action against the perpetrator. Process tracking can be a lifesaver if there is an employee within your company is making illegal use of company data.

Even though it is extremely important to audit certain administrative accesses, it is also important to audit policy changes. Intruders often make auditing policy changes. When a person outside your organization is able to break into your network, often times they will change your auditing policies. For example, if an intruder is going to gain access to

your network, they often attempt to turn off the account logon auditing policy. In another scenario, the intruder may also want to access secured data. It would be in the intruder's best interest to turn off the policy that sets auditing objects such as folders.

It is also possible for people within your own organization to use secured or confidential data with malicious intent. Take for example a banking institution. Banks hold every piece of information you would need to use an account holders banking information for your own benefit. The banks personnel may have access to change auditing policies on a secured "accounts" folder. It is then impossible to see who is accessing this data. When a company does not know who is accessing their secured resources, they are at a severe security risk. We see the unfortunate results all the time of stolen identity and most frequently this stolen data comes from banking or lending institutions.

Another way an intruder can manipulate or hinder your auditing policies is by changing who has access to audit information or logs. By auditing privilege use, you can track any changes made to the permissions for viewing audit logs. This can also be a crucial piece of information to audit. Often times the IT (information technology) department of an organization knows much more about computers than management. Just because you have IT professionals working for you does not in any way mean that they will not eventually work against you. There have been many cases where IT professionals have stolen secured company data for their own illegal use. If an IT professional were to change the permissions so that systems administrators were unable to view their audit logs, it would be possible that, at least temporarily, that person would be able to access the secured data without being caught. Eventually, once the system administrators had regained access, they would be able to view the data and catch the perpetrator.

It may also be important to track who is loading software on your machines. Unauthorized software may cause system problems which are unable to be fixed because the software is not supported by your organization. You are able to audit the loading of unauthorized software by adding an audit option for "Create Subkey" under HKLM\SOFTWARE or HKCU\SOFTWARE in the Registry (Robichaux, Paul. Managing the Windows 2000 Registry. Sebastopol: O'Reilly & Associates Inc., August 2000. Page 146).

Using Aelita InTrust Software For Security Auditing:

As I discussed previously, generally audit logs are stored in files on network drives. This method of saving logs is effective for smaller organizations with a small amount of users and secured data. If the audit information is saved to a log for an extended period of time, it can become somewhat difficult to track information that may be necessary and vital to the successful conclusion of a security violation investigation. It is recommended that these logs are reviewed frequently to ensure that resources are not being accessed illegally. Typically it would be beneficial for the person reviewing the logs to have the ability to sort by specific log information such as the date, source, or user of the event.

This sorting option would make larger organizations much more efficient. In reviewing their security logs.

Fortunately a company called Aelita has developed a software solution named InTrust to assist systems administrators in the storing and organization of their audit information. In addition to the benefit of organization, InTrust also allows this data to be archived for an extended period of time. The longer the data can be stored, the better. Organizations occasionally find out about a security issue after vulnerability is overlooked. Systems administrators are then able to go back and review their audit details to ensure that there has been no unauthorized access to a system or object.

Aelita's InTrust software has the ability to audit and keep logs for all the security events I discussed previously. I must note that when tracking account logon events, this must be activated from directory services. In order to fulfill the requirements of InTrust, you are unable to use the Event Viewer to track logon events. Remember, Event Viewer's security feature saves logon information on that machine only; it is not stored on a shared network drive.

Aelita has a reporting console that enables system auditors an easy way to view audit information. The reporting console is organized in an easy-to-read manner that gives you a clear and concise audit report, rather than scrolling through text files. The reporting console allows information to be divided by workstation therefore you are able to see clearly all the logon attempts, for example, on a particular computer. Aelita's web site points out an important note and a big argument in favor of their reporting console. Not only can you see the logon activity for a particular machine, it is also organized in such a way that you are able to actually analyze the data. For example, if you see several unsuccessful logon attempts in a row, then all of the sudden you have a successful logon, which could potentially indicate hacker activity. You would definitely want this information stored in an easy to read and analyze manner.

For larger corporations it is not always easy to have somebody review audits constantly. This can be a rather monotonous task that can cost large businesses a lot of money. Aelita Journal gives the option of notifications of certain types of events. Say for example that you have an extremely secure folder on your network drive that hold the names, addresses and credit card numbers for you company's customers. With Aelita Journal you can receive a notification via e-mail, pager, or network message that a user is attempting to access that folder illegally. This ability enables the system auditors to review the reporting console immediately in order to find out who is attempting to access the data.

Auditing Recommendations:

Now that I have given you examples on what types of security audits can be done, let's look at some recommendations from the National Security Agency (NSA). The NSA points out the importance of continually auditing the event log. It is pointed out that the event log is the most critical point of determining unauthorized systems access. Again, as stated above, the event log is capable of logging events in which a user or nonuser

attempts to log on to a workstation without access. The NSA also recommends that these logs are checked daily or weekly to ensure that security auditors have the violation information as quickly as possible. It is important to realize that a key to keeping intruders off your workstations is to find out who they are, recognizing their presence and taking steps to ensure they are unable to successfully gain access to secured systems or system resources.

In addition to expressing the importance of the systems event log, the NSA has also determined a way to have permissions set on the log itself. The NSA recommends that, "An auditors group may be created and given full permission to that log." An important note is that, "Only individuals without administrator duties should be given access to that log." This policy would give only the system auditors exclusive permission to the event log. As described above, it is very important to ensure that your administrators do not have exclusive access. Please remember as I have stated several times before that system perpetrators do not only come from outside of your organization. Each company has a very intelligent source of IT professionals that could cause more harm than good if they so desired.

The NSA also points out another important security concern in corporations and that is the physical access to system resources. Much of my auditing explanation has taken a look at systems auditing, but I have not explored the importance of physical security. Securing our system resources is one of the most important parts of our security framework. For example, you would not keep a production server in an unsecured room where just anybody could tamper with it would you? The NSA recommends the following guidelines for securing your physical system resources:

- Keep servers in a secured room
- Disable the removable media based boot option if available
- Remove removable media drives if not required, or install a locking device
- The CPU base should be secured by a key stored safely away from the computer
- Refer to system documentation to implement a systems bios password.

In addition to the auditing recommendations listed above, the NSA also recommends that audit logs are reviewed, stored and cleared every day or week. Audit logs can use a large amount of system resources that my cause system problems if audit logs are not reviewed and cleared in a timely manner.

Physical Security Recommendations:

Now that we have taken a look at some recommendations from a systems audit point-of-view, I would like to touch on the importance of physical security audits. Up until this point I have given you an explanation of security audits that can be done on a computer, I would highly recommend not only performing the above audits, but performing a physical security audit of your computers as well.

In many companies, employees use laptops instead of desktop workstations. It is important to make sure the laptops are secured at all times to ensure minimum

vulnerability of theft. In many cases, when a laptop computer is stolen, it is not the cost of the hardware that is the main concern of the company; it is the cost of the information stored on the computer. In order to offer a secure solution for laptop users, docking stations are recommended. Docking stations allow security by providing a lock and key mechanism.

I know you may be thinking, okay, my computer is docked and I'm good to go. Well, the first question I would have is, what did you do with your keys? First off, did you remember to remove them from the docking station? And secondly, did you put them in your desk drawer? It is scary to think of how easy it is to leave your computers unsecured when you are busy or running late. It can happen without you even thinking about it. Leaving keys in obvious places does nothing to eliminate security risks. It only takes a few seconds to look around your desk for a key.

Random security audits by management can help employees recognize when they are at risk for theft of hardware. By visiting employee's desks, unannounced, managers can see who is in compliance with their systems physical security. It is also important that management coaches employees whom are not in compliance and make it known that disciplinary action can be taken on repeat offenders. Keep logs of these offenses so you know of your employees that leave themselves vulnerable to theft.

Not only do we need to think about confidential data that is located on workstations, we also need to think about the paper documents that are in our desks and file cabinets. Making sure that file cabinets are locked, and again that key's are not in obvious places, are another part of the security audit that should be completed by management. Even scarier is the fact that confidential paper documents can be stolen more easily and without you even knowing it. For instance, an employee could simply find the key to your file cabinet, open it up, take some documents and make copies. You may never know that the documents were stolen because that employee can return the originals to your desk and put your key back exactly where you found it. Just think for a moment about the vulnerability that is exposed if you keep confidential paper documents unsecured.

Summary:

In summary, I have explained the importance of performing periodic security audits. These audits, even though periodic, should be performed quite frequently to ensure that your systems are not vulnerable to intrusion by people with malicious intent. It is important to identify perpetrators who are gaining unauthorized access to your systems and system resources such as applications and secured documents. Detecting this intrusion will assist you in finding ways people are gaining access to your systems and help you find ways to ensure your resources are secured.

I have also explained to you how to get your systems ready for performing audits. It is important to note that auditing is something that cannot be performed without first taking steps to enable auditing. If these steps are not taken you are unable to audit detailed system events that will identify perpetrators.

In addition to explaining the importance of security audits and how to get your systems ready to perform security audits, I have also explained several different audits you can perform. It is important to note that not only is it necessary to perform audits on your systems, such as auditing the event viewer and registry, but it is also necessary to perform physical security audits to ensure that your systems are not vulnerable to theft.

When tracking security audits, typically they are stored in log files. These files can take up a lot of systems storage which may prevent you from having adequate drive space for other necessary documents or applications. I have given you an option offered by Aelita which will allow you to track audit events easily and allow you to search for unauthorized event more efficiently. Aelita Journal also offers you a storage option that will not take up as much drive space as the audit logs that are typically stored.

Finally, I have explained some auditing recommendations made by the NSA. The NSA is a good resource to look for security information and ways to prevent network or system intrusion. They offer many recommendations about both systems and physical security than can help you prevent security vulnerabilities within your organization.

I am in hopes that this auditing review has been helpful and will assist you in audits of your systems. I feel auditing is an important part of ensuring systems stability and availability. If you do not perform random security audits, you may be missing intruders that are breaking into your systems with malicious intent.

References:

1. Osborne/McGraw-Hill. Windows NT Server 4.0. Berkeley: Brandon A. Nordin, 1998. page 56

2. "Audit Active Directory Objects In Windows 2000." 6 June, 2003, URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q314955

3. "How To Enable and Apply Security Auditing In Windows 2000." 3 June 2003. URL: http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q300/5/49.ASP&NoWebContent=1

4. "InTrust (Formerly EventAdmin) Features and Benefits." URL: http://www.aelita.com/products/intrust/intrust_benefit.htm

5. Mathers, Todd. "Security and Auditing" 12 November 1998, URL: http://www.informit.com/content/articlex.asp?product_id={BA00ED43-CEF4-4B2B-B120-5DE3837721A5}&element_id={F6BDCDB5-FE5D-4C2A-A8C0-CAB366169413}&st={EEA4B8BA-4464-4E41-BE37-B668A7ACCF61}&session_id={6CF034F0-3D92-4C24-A9C2-59F86BB70674}

6. "Local Policies" URL: http://rmeservy.byu.edu/isys648/rights/policyoptions.htm

7. McGovern, Owen R. and Haney, Julie M. "Guide To Securing Microsoft Windows 2000 File And Disk Resources." Version 1.0. 19 April, 2001. URL: http://www.nsa.gov/snac/win2k/guides/w2k-8.pdf

8. Robichaux, Paul. Managing the Windows 2000 Registry. Sebastopol: O'Reilly & Associates Inc., August 2000. Pages 141 – 149.