AUDITING AS PROTECTION AGAINST SYSTEM ERRORS

STEGĂROIU CARINA-ELENA,
LECTURER PHD, „CONSTANTIN BRÂNCUŞI" UNIVERSITY, TÂRGU JIU, ROMANIA
carinastegaroiu@yahoo.com

Abstract

Auditing is an instrument that can be used to improve the security of any systems in our network.

In case of a security breach or network penetration, the event recording log that we can find on different logl files helps us identify what has been compromised and the person who has perfoemned the operations.

Auditing should not be considered a 'configure and forget' type of operation, but a periodic review of the log file in order to look for unsual events. This would help discover a minor breach before the intruders cause more trouble in our network.

Key words: *information security, auditing, internet, firewall*

JEL Classification : *A10, B23, C61*

1. Introduction

Auditing represents the background of any security protocol, as the log files only communicate what happened and do not ensure a secure system.

The security protocols ensured by the operating systems in order to limit the access to important resources must be used, so that in the event of someone trying to illegally access the system, they would have to use superior knowledge to endanger the system and gain unwarranted information.

The software provider that creates an application can choose to implement the registration option for their product, but, as security is vital, such things must be taken into consideration when we evaluate different products [1].

If the log registration is needed, we can study the afferent documentation in order to discover the way in which this application is implemented..

For example, the following set of questions can be asked in the case of an application that is running under UNIX: does the programme create and run its own log file? Is the UDP154 port sending messages to syslog? Can you pinpoint the location of the log file? The same queries are valid for an application written for Windows NT: does the product create its own log file or does it use Event Logging? The ability to control the location of a log file which is specific to an application is important, especially when installed on a vulnerable host. Directing the exit data from the log file to a read-only file can help us protect against any foreign modifications.

The safety of a well configured firewall should be used as an excuse to neglect regular check-up procedures regarding security. Even if we trust the users in our local network – which is not necessarily a good idea – we should not blindingly trust our firewall to protect us against all the possible external threats. The Internet allows a hacker to attack a LAN network virtually from any place on the globe. There are programmes on the Interned that automatize the search and penetration process of vulnerable systems and networks. After installing and configuring a firewall, we should think it a first line of defence and not a complete solution.

When we talk about auditing – the process of recording certain events that happen on computer or network – it is important to understand that this is the only way to detect the source of a potential compromising of the network. We can easily find out if a malicious perpetrator is capable of destroying important data or block an important server. But can we determine the cause? For example, in the event of a server block, how can we be sure that it was not a programming error in the operating system? Is it possible that the error is caused by a newly installed application? Or is the person responsible within our ntweork or are they operating from the exterior?

Both UNIX, and Windows NT have extended auditing capabilities. However, we cannot be sure that the installation of the operating system will generate the list of audited events that will prove most useful.

In the following paragraphs, we will touch on these aspects, the types of information we can uncover and the configuration of the auditing functions provided by these systems.

2. The importance of auditing the network security.

The worst situation regarding the security of a network is that in which a breach occurs without our knowledge. The longer a hacker is attached to the systems in our network, the greater the damage will be. We are not talking only of the initial damage – sensitive information theft or destruction of important data – but also of the time we are granting the hacker to plant the germs of a future infestation. As long as we are not aware of the hacker's presence, he can replace important programmes in the system with modified versions. They can create user accounts or secret passages into the network, so that when the hackers's presence is detected, the network is already in a mess that will need a major cleanup. This is why, besides the auditing and logging options of our firewall, we should keep under strict surveillance all the operating systems installed on the every computer in the network. To this purpose, we should instruct ourselves regarding the techniques that can be used and implement them in their full version. Also, the data which resulted from auditing techniques should be analysed quite often.

There is no point in using extended auditing techniques if we don't set a regular review of the log files. The study of large files used to log events can take a lot of time and it is often easy to gloss over this task if you have a difficult day. It's not always necessary to read every event in the log of the Windows NT system or in the large files created with the syslog function in UNIX.

Here are some things that must be taken into consideration when dealing with log files:

- If a breach in your system is possible, then how can we be sure that the log files haven't been compromised? Can you trust the information in your log files? If the intruder used a "root" account, they have the ability to edit the log files to wipe their tracks.
- It is easy to become superficial when performing a routine task. How careful are we when we need to go over several boring log files every day? It is possible that after months or years of reading files without any significant discoveries to overlook an important recording that could uncover a security breach.
- Log files can become very large. It is tempting to erase them or even restrict the types of events that can be logged, so that we don't have to worry about free space on your disk.

The certainty that the information in a log file are correct can be misleading, but in most cases, these are the only data we can use when we try to find the source of a breach. If the budget allows, we can solve this problem by placing the log files on a write-only unit. The price of the CD-ROM and other units that are not rewritable has gone down in the last few years, so such an expense can be easily justified to the management. This technique does not protect against incorrect, corrupted programmes. If an intruder has managed to replace the important files in a systems that write within the log files, we can still have a problem. But this technique prevents the intruder from editing a log file in order to breach the network.

Security is a vital task. We should not leave it in the hands of only one person and in order to overcome the problem of boredom that can occur when reading log files, we can do more things.

Firstly, we can use instruments that are designed to consolidate or look for certain information in the log files.

Secondly, we should delegate the review task to several people. This activity should be dealt with over several days, so that the boredom factor doesn't have such an impact.

The administrator should frequently check the auditing and review processs. Having only one person in charge of reviewing sensitive security information is potentially a security problem in itself. It is better to trust two or more people with such a task.

It is also better to produce large log files, which contain a variety of events, than to select only a few events which we think might present a problem.

For example, in Windows NT we can opt to audit the successful and unsuccessful log-in operations [2]. Although auditing failure to connect events may not produce as large a number of recordings as the auditing the successful log-ins which would entice us to keep a smaller event log, successful log-ins recordings could be a valuable instrument in determining how, when and why the security system of our network was breached. The high number of unsuccessful log-ins could indicate that someone is trying to access the network by guessing passwords and this should trigger a warning. Successful log-ins can show us when a user account is accessed outside working hours or from an unsanctioned computer.

We consider the data from log files as important as the most sensitive information within your network. We do not regularly erase log files to free space on the disk. If we do not use write-only units, which can be easily stored for future reference, we can make backup copies of the log files on offline units for an undefinite period. When there is a security breach, we may discover that this has occurred as a result of Trojan placed

within the system months or years ago. It is advisable that log files be kept so that they may be carefully analysed later on if need be.

3. Protecting log files resources in UNIX

Because UNIX has a revolutionary past in which different authors have contributed, in time, with different components, there are various log files that can be useful in the reviewing process.

To automate the processes on a UNIX system, the cron daemon is used. This daemon allows you to create script files that can be run at specific times and dates, without the user's intervention. Although most of the modern implementations of this daemon use the syslog facility, there is a log file called var/log/cron. Hackers who can manipulate the configuration file of the cron daemon can programe the process to run in order to gain access to the system and to higher privileges. Both the cron configuration file and the log file must be reviewed regularly and it is best to configure the syslog daemon to take care of this auditing [3].

Although it does not use a log file, the **ps command** can be as useful as a log file when we are investigating a possible breach of security.

Instead of the data in the log files, the ps command uses the process table in the UNIX nucleus and displays information on current processes. If an intruder has managed to enter the system and has launched a background programme, we can use this command to look for them. Because the information is coming from the nucleus and not the log file, there are few chances of them not being correct. Depending on the UNIX version, the ps command can give us the following information:

- The process identifier
- User name
- TTY (the user terminal)
- Start time
- The current command
- The in-use percentage of the processing central unit
- The in-use percentage of the memory
- The time when the process began

By using this command and comparing the results with the content of the above mentioned file, we can identify suspicios processes that would warrant further investigation. We are also looking for processes that are running for a longer time than normal, during times when they are not supposed to run or that are run by an unauthorized user.

Unlike UNIX, the Windows NT operating system allows the auditing of a large number of events and we only have to use Event Viewer to view the messages created. This programme only works for the operating system.

There are certain applications that update log files besides writing within Event Log files. There are also applications that can run one or both auditing activites, depending on the way they have been programmed.

Event Viewer is found in the Administrative Tools folder and it is used to analyse the events audited by the Windows NT operating system. To keep the recording three different log files are used, and we can select what file to view:

- System – events that have to do with the operating system, such as turn on, turn off, device malfunction.
- Application – registering applications;
- Security - the events related to security problems which have been chosen for auditing.

While the log files System and Application can be useful for troubleshooting, Security contains the events we have chosen for auditing.

By using Event Viewer, we can configure the way in which the events are stored in files and we can export the data in a file that can be opened with an application using a table-like operation or with another type of programme. To save the recordings in a text file – ASCIII with a comma delimitator, we select Save As from the Log menu. Next we select the Comma Delimited Text option from the Type box. When a log file increases, we can use this method to save it and clear it by using the Clear All Events option from the Log meny. To manage the size of the log file, we can use the Settings option in the File menu.

4. Conclusions

Auditing is an instrument that can be used to improve the security of any systems in our network [4]. In case of a security breach or network penetration, the event recording log that we can find on different logl files helps us identify what has been compromised and the person who has perfoemned the operations. Auditing

should not be considered a 'configure and forget' type of operation, but a periodic review of the log file in order to look for unsual events. This would help discover a minor breach before the hackers cause more trouble in our network.

Nowadays, using computers and IT programmes has become a vital element in the informational system of a company. Once the new technologies were introduced in the operating, transmitting and storing of data processes, a series of threats and vulnerabilities have begun affecting the information system.

That is why managers must deal with guarateeing the fairness and security of the operations within the information systems and converging these objectives with the organizational strategies.

To counterattack these negative aspects information control procedures have been implemented within every unit. These objectives and internal control procedures aim to ensure the security of the data systems and reduce the risck of threat and vulnerability within the system.

In the Romanian specialised literature and practice, we can find terms such as auditing informational systems, auditing information systems or IT auditing. The conceptual difference is given by the content and level of auditing, on one hand and on the other hand by the conceptual difference between the informational system and the information system. Therefore, auditing the informational system is the conceptually broader term, covering all levels of the system in question, from evaluating the design and use of the IT system to evaluating the security policies and procedures at an operational and strategic level.

Auditing the information systems, the IT auditing, covers only the IT system. It refers to the evaluation of IT risks threatening the physical security, the logical security, the management of change, the contingency plans etc. Generally, the IT auditing represents a range of IT processes that answer a client's specific need.

The main types of IT auditing are:

- Auditing the operating system – reviewing computer and network operational systems, at different levels: operating systems, network, application software, database;
- Auditing IT installations – refers to the physical security, work environment checkups, management systems and IT equipment;
- Auditing the developing systems, referring to project management checkups, the specifications, development, testing, implementing and operations technical and procedural controls;
- Auditing IT management – includes reviewing the organization, structure, strategy, work planning, resource planning, budget setting, cost control etc.

5. References

[1] **Oprea D.**, *Protecţia şi securitatea informaţiilor*, Ediţia a II-a, revăzută şi adăugită, Editura Polirom, Iaşi, 2007.

[2] **Mihai I. C., Popa I. F.**, *Securitatea în Internet*, Editura Sitech, Craiova, 2008.

[3] **Popa S. E.**, *Securitatea sistemelor informatice*, note de curs şi aplicaţii pentru studenţii Facultăţii de Inginerie, Universitatea din Bacău, 2007.

[4] **Senft S., Gallegos F**., *Information Technology Control and Audit*, Auerbach Publications, 2009.