Journal of Applied Business Information Systems

http://www.jabis.ro

Windows and Linux Security Audit

Sergiu Miclea*

* Master Student at Master in Business Information Systems, West University of Timisoara, Faculty of Economics and Business Administration, Timisoara, Romania

Abstract: *The security audit in operating system is necessary, especially when there are multiple users using it or when the system is part of a company's network. Before heading into the security audit, you have to be aware of the fundamentals of IT security auditing, whose main objective is to assure protection of the information assets and to dispense information properly to authorized parties. In order to make the best choice when choosing an operating system and security is the most important factor, you have to know each operating system' procedures for creating, logging and reporting of security audits. Finally, it is necessary to make a list comparing the most important security features of the operating systems and choosing the best solution based on it.*

Keywords: *Security, Audit, Windows, Linux, OS, Comparison, Logging.*

1. INTRODUCTION

In [6], client computers are the source of more the attacks and vulnerabilities than any other computer in an enterprise. They are often left out from audits due to lack of time, money and other resources.

The reason why client computers are neglected in the audits, even though they are use for attack or are attacked more than servers and they make a substantially higher percentage of overall computers in a network, is because clients don't house the data and applications, so they are ignored in lieu of servers being the target for audits.

My objective is to give a new perspective on how the clients should be perceived so they can be incorporated in to the audit, making the overall security and stability of the network dramatically increased. If the security control points, scope of clients and target goals are understood, then the audit should go smoother and faster.

Comparisons between Microsoft Windows and Linux operating systems have been a much debated subject when discussing about personal computer and server industry. Windows is known for retaining its extremely large sales over other operating systems, while Linux sustains its status as the most obvious choice of free software operating system.

A true comparison of security between the two operating systems is difficult to obtain and it is a subject vehemently discussed between security professionals and hobbyists.

So, another objective is to identify what exactly are the main differences between Microsoft Windows and Linux, in terms of security, by studying different factors like malware, open or close, response speed, user accounts, file system permissions. If the k measurements are made by two groups independently, will get two tables, each having k lines and m+n columns. The lines correspond to the k measurements and the columns correspond to the m resultative variables Y_1, Y_2, ..., Y_m and the n independent variables X_1, X_2, ..., X_n.

In [10], there are a few items that constitute the most common security parameters that can be evaluated in an operating system such as:
- password rules (like length, history, required)
- password aging
- lock-out on unsuccessful logins

- login station and time restrictions
- logging of certain events
- access privileges
- network security

2. INFORMATION TECHNOLOGY AND SECURITY AUDIT FUNDAMENTALS

In [3], IT audit constitutes of an examination of the controls within IT infrastructure. The review obtained from the evaluation gives information regarding certain aspects such as safeguarding assets, maintain data integrity and effective operation in order to achieve the company's goals. The evaluation can be performed in conjunction with financial statement audit, internal audit.

The purpose of IT audit differs from financial statement audit, because the latter is adhering to standard accounting practices, while IT audit evaluates the system's internal control design and effectiveness. This may include efficiency and security protocols, development processes.

The main objective is to assure protection of the information assets and to dispense information properly to authorized parties.

In [2], information security audit is an audit on the level of information security in an organization.

The information security audit's processes are:
- Audit planning and preparation - The auditor should be adequately educated about the company and its critical business activities before conducting a data center review. The objective of the data center is to align data center activities with the goals of the business while maintaining the security and integrity of critical information and processes.
- Establishing audit objectives - The next step in conducting a review of a corporate data center takes place when the auditor outlines the data center audit objectives. Auditors consider multiple factors that relate to data center procedures and activities that potentially identify audit risks in the operating environment and assess the controls in place that mitigate those risks.
- Performing the review - The next step is collecting evidence to satisfy data center audit objectives. This involves traveling to the data center location and observing processes and procedures performed within the data center.
- Issuing the review report - The data center review report should summarize the auditor's findings and be similar in format to a standard review report. The review report should be dated as of the completion of the auditor's inquiry and procedures.

In [8], a computer security audit is a manual or systematic measurable technical assessment of a system or application.
- Federal or State Regulators - Certified accountants, CISA. Federal OTS, OCC, DOJ, etc.
- Corporate Internal Auditors - Certificated accountants, CISA.
- Corporate Security Staff - Security managers, CISSP, CISM.
- IT Staff - subject matter experts, oversight support.

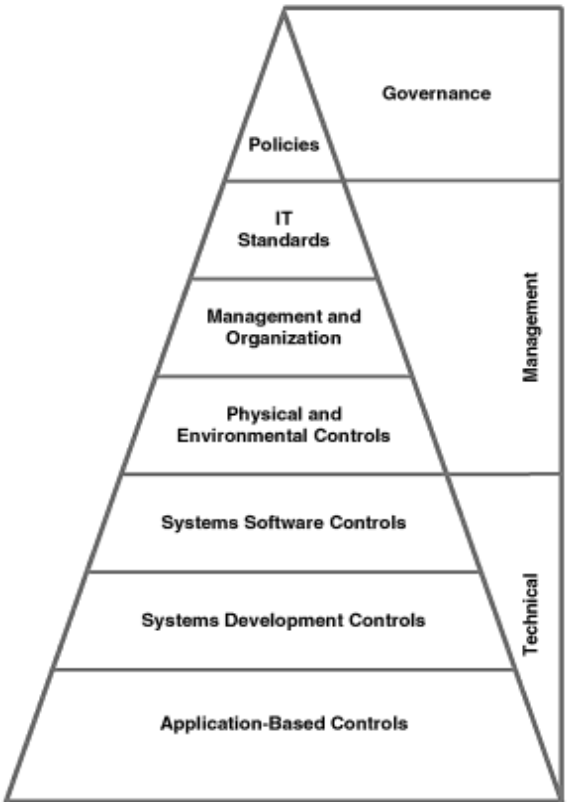

Figure 1. IT General and Application Controls Hierarchy

An appropriate way of looking IT General (which covers all information systems operation), can be seen in Figure 1 describing the IT controls hierarchically. At the top of the triangle are IT policies defining the overall enterprise IT organization. Moving down the Figure 1

hierarchically are general controls for IT standards, organization of the IT function, and physical and environmental controls. The next level down groups two of the technical-level general controls: systems software controls and systems development controls and at the base of the triangle are the application-based controls.

3. MICROSOFT WINDOWS SECURITY AUDIT

In [12], there is a lot of auditing enhancement in Microsoft Windows Server 2008 R2, but also in Windows 7. These enhancements improve the level of detail in security auditing logs and simplify the deployment and management of auditing policies. Among the enhancements there are:

- Global Object Access Auditing. The administrators of Windows Server 2008 R2 and Windows 7, can define SACLs (system access control lists) for file system or registry. These control lists can then be applied to every object of that type. This feature can be used to verify if critical files, folder, registry settings are protected, but it also can be used for identifying when an issue with a resource occurs.
- "Reason for access" Reporting. ACEs (access control entries) provide the privileges on which allowing and denying access to an object decision was based. This can be used for the documentation of permissions, which allow or prevent the occurrence of a particular auditable event.
- Advance audit policy settings. There are more than 50 new settings that can be used instead of the nine basic auditing settings (which can be found in Local Policies/Audit Policy) to allow administrators to more specifically target the types of activities they want to audit and eliminate the auditing activities that are not necessary that can make auditing logs difficult to manage and decipher.

In Windows Vista, but also in Windows Server 2008, the number of auditable events has increased from nine to 53. This enabled administrators to be more selective in the number and types of events to audit. The new auditing events are not integrated with Group Policy, however, and can only be deployed by using scripts with the Auditpol.exe tool.

Windows Server 2008 R2 and Windows 7 integrated all auditing capabilities with Group Policy. This allows administrators to use GPMC (Group Policy Management Console) in order to configure, deploy and manage these settings. These new systems allow IT professionals to track when precisely defined, significant activities take place on the network.

These enhancements made to Windows Server 2008 R2 and Windows 7 allow administrators to connect business rules and audit policies. Administrators can apply audit policy settings on a domain and document the compliance with rules such as:

- All group administrator activity with finance information
- Track files that are accesses by a per-defined group of employees.
- Verify if the correct SACL is applied to every object when it is being accessed.

The enhancements support the needs of IT professionals responsible with the ongoing security of an organization's physical and information assets.

There are a few considerations to take into account with auditing enhancements in Windows Server 2008 R2 and Windows 7:

- Create an audit policy. If you want to create and advanced Windows security auditing policy, you have to use GPMC or Local Security Policy.
- Apply audit policy settings. Client computers must run Windows Server 2008 R2 or Windows 7. These are also the only systems that can provide "reason for access" reporting data.
- Develop an audit policy model. You must use GPMC targeting a domain controller running

	Windows XP	Windows Vista	Windows 7
Categories of security auditing events that can be monitored	9	53	53 (integrated with Group Policy)

Table 1. Evolution of security auditing categories in Microsoft Windows

In Table 1 can be seen that Windows XP had nine categories of security auditing events that could be monitored for success, failure or both. These auditing events have a broad scope; some actions can generate a large number of event log entries.

Windows Server 2008 R2, in order to plan advanced security audit settings and global project access settings.
- Distribute the audit policy. The GPO (Group Policy Object) can be distributed by using domain controllers running Windows server operating system.

The advanced audit policy settings can be applied to systems running Windows Vista, but they must be created and applied separately by using Auditpol.exe log-on scripts.

The basic audit policy settings and the advanced settings must not be combined, as they may cause unexpected results.

In [13], to enable Windows Security Auditing on a system prior to Windows Vista and Windows 7 (Windows 2000 and Windows XP) you have to follow the steps:
- Log-on to Windows using an administrator account.
- Ensure the Group Policy snap-in is installed.
- Click Start, point to Settings and then click Control Panel.
- Double-click Administrative Tools.
- Double-click Local Security Policies to start Local Security Settings MMC snap-in.
- Double-click Local Policies to expand it, double-click Audit Policy.
- In the right panel, double-click the policy that you want to enable or disable.
- Click the Success – an audited security access attempt that succeeds, and Fail – audited security access attempt that fails check boxes for logging on and logging off. For example, if a user tries to access a network drive and fails, the attempt is logged as a Failure Audit event.

The domain-level settings override the local policy settings. If Active Directory is enabled, administrators can monitor access to Active Directory.

Connecting to the internet exposes anyone at risk. Someone could try to access a system and if there are not enhanced security measures, the hacker could steal confidential data. Account auditing gives the administrator the possibility to see who tries to break into a specific account. Whenever someone tries to access a system, an event is triggered when the access attempt was successful or failed. With account auditing settings these events can be logged by the system and the administrator is able to these log files at any time to see if the system is being accessed unauthorized.

In [14], to enable account auditing on Windows 7, one must start secpol.msc tool, by using the run command from the start menu. The Local Security window will be displayed. Navigate to Local Policies, then Audit Policy and right click the Audit account log-on events policy option and choose Properties, as seen in Figure 2.

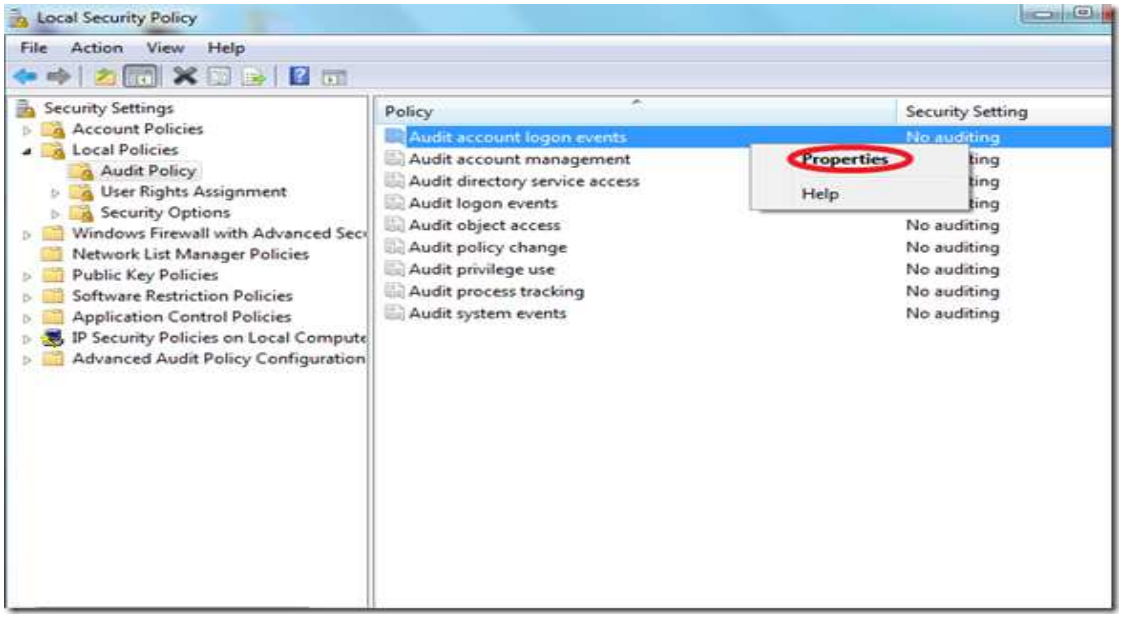

Figure 2. Accessing the properties of Audit account log-on events

Check the check boxes corresponding to Success and Failure as seen in Figure 3. By setting them both on, the operating system will save the logs of both successful and failed attempts.

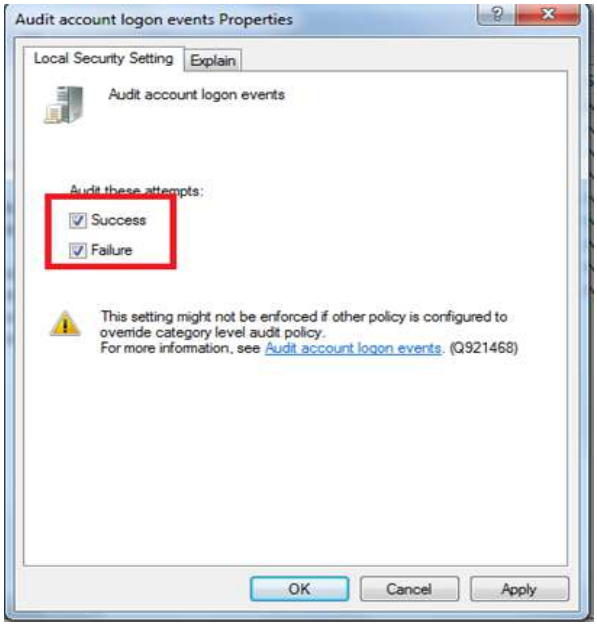

Figure 3. Settings for auditing the attempts

After the administrator follows the same procedure for Audit log-on events, he can see the logs of the log-in attempts with Event Viewer. To access the Event Viewer, search for "event viewer" on the Windows 7 start menu. In the Event Viewer, navigate to Windows Logs, then Security option and he can see the logs for both the successful and failed log-on attempts.

4. LINUX SECURITY AUDIT

Before getting into Linux security audit, I would like to point out the Linux operating system architecture. The architecture diagram as seen in Figure 4 is made of:

- Linux kernel – the code that connects the user application and system hardware.
- Hardware controllers – these are used by the kernel to interact with the hardware.
- Operating system services – this is software, excluding the kernel, which is considered part of the OS. For example: X Windows system, command shell.
- User applications – software other than the kernel and operating system services. For example: word processors, browser, and multimedia applications.

The best choice for auditing file events in a Linux operating system is to use the audit system of kernel version 2.6. Modern versions of Linux (2.6 and up) come with "auditd" daemon. This tool is responsible with writing audit records to the disk. When the tool starts up, it reads the rules specified in /etc/audit.rules. The administrator may open this file to make changes.

For a successful audit procedure the administrator must use some utilities like these ones:

- auditctl – this utility helps with the controlling of the kernel's audit system. Using this tool, the administrator can get statuses, add or delete rules from the kernel audit system.
- ausearch – using this command the administrator may query the audit daemon logs for events based on the specified search criteria
- aureport – this tool is used for viewing reports generated based on the audit system logs.

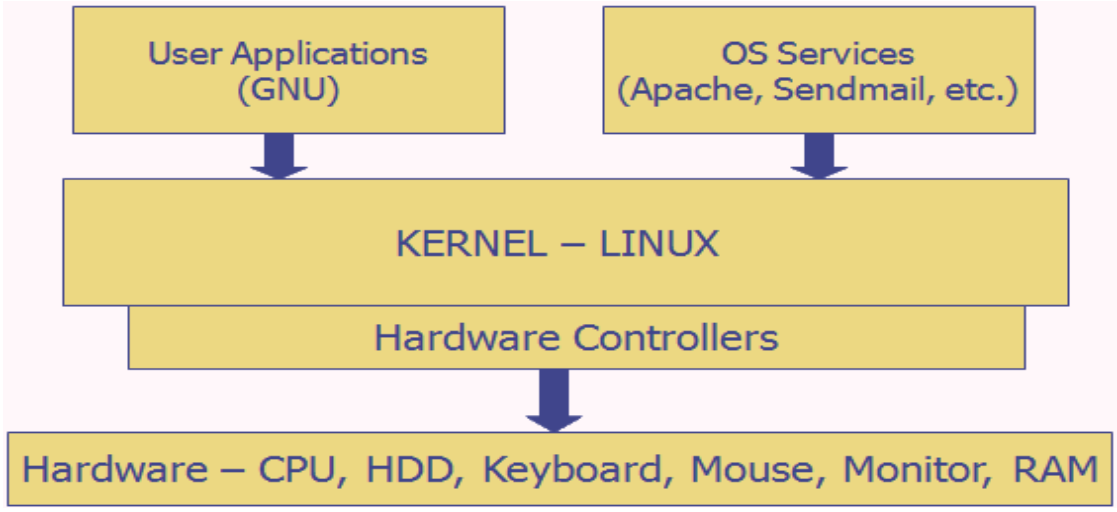

Figure 4. Linux architecture diagram

Before any auditing, it is necessary to install audit package, which contains the user utilities for storing and searching the audit records generated by the audit subsystem. These steps apply to Linux 2.6 kernel subsystem. CentOS or Red Hat and Fedora Core includes rpm package. To install the package, the administrator must use "yum" or "up2date" command. For example: "# yum install audit" or "# upd2date install audit".

To configure the "auditd" service to start on boot, the administrator must use the command "# ntsysv" or "# chkconfig auditd on".

The command "# /etc/init.d/auditd start", starts the auditing service.

The next steps should be setting a file for auditing. For example, if the administrator would like to audit a /etc/passwd file, he would type the following command: "# auditctl –w /etc/passwd –p war –k password-file.

- -w /etc/passwd – is used to insert a watch for the file system object at given path, in this case the passwd file.
- -p war – is used to set permissions filter for a file system watch. Other examples are "r" for read, "w" for write, "x" for execute and "a" for append.
- -k password-file – is used to set a filter key on passwd (watch). It can uniquely identify the audit records produced by the watch. When searching audit logs, the administrator must use password-file string or phrase.

So, with all these commands, the administrator is monitoring a /etc/passwd file for anyone (including the "syscall") for write, append or read operations on a file.

Another example is "watching" on etc/shadow with the arbitrary filterkey "shadow-file" that can generate records for reading, writing, executing and appending to "shadow":
auditctl –w /etc/shadow –k shadow-file –p rwxa

The next example suppresses auditing for mount syscall exits:
audit –a exit,never –S mount

In the next example, the command adds a watch "tmp" with a null filter-key that generates execute records on "/tmp". This command is especially used on a webserver:
auditctl –w /tmp –p e –k webserver-watch-tmp

The next command allows an administrator to see all the system calls made by a program called "sshd", which has the process id pid – 1005:
auditctl –a entry,always –S all –F pid=1005

When the administrator needs to find out who accessed a file, for example /etc/passwd, he needs to run any of the commands:
ausearch –f /etc/passwd
ausearch –f /etc/passwd | less
ausearch –f /etc/passwd –i | less

The command "-f /etc/passwd", does a simple search for the specified file. The parameter "-i" is used to interpret numeric entries into text. For example, an unique identifier can be converted to an account name.

Running the commands generates the following output:
type=PATH msg=audit(03/16/2007 14:52:59.985:55) : name=/etc/passwd flags=follow,open inode=23087346 dev=08:02 mode=file,644 ouid=root ogid=root rdev=00:00
type=CWD msg=audit(03/16/2007 14:52:59.985:55) : cwd=/webroot/home/lighttpd
type=FS_INODE msg=audit(03/16/2007 14:52:59.985:55) : inode=23087346 inode_uid=root inode_gid=root inode_dev=08:02 inode_rdev=00:00
type=FS_WATCH msg=audit(03/16/2007 14:52:59.985:55) : watch_inode=23087346 watch=passwd filterkey=password-file perm=read,write,append perm_mask=read
type=SYSCALL msg=audit(03/16/2007 14:52:59.985:55) : arch=x86_64 syscall=open success=yes exit=3 a0=7fbfffcb4 a1=0 a2=2 a3=6171d0 items=1 pid=12551 auid=unknown(4294967295) uid=lighttpd gid=lighttpd euid=lighttpd suid=lighttpd fsuid=lighttpd egid=lighttpd sgid=lighttpd fsgid=lighttpd comm=grep exe=/bin/grep

In the output "audit(03/16/2007 14:52:59.985:55) ", shows the audit log time. The line "uid=lighttpd gid=lighttpd" shows the users in numerical format. If the administrator chooses to use "-i" option, the numeric data can be converted to a more approachable format. In this

example, the user is "lighttpd" and he used the "grep" command to open a file.

The output, shows on line "exe="/bin/grep"" that command "grep" was used to access /etc/passwd file.

The "perm_mask=read", tells us that a file was open for reading.

The log files can give a clear idea to the administrator who read the file using the "grep" command or made changes using vi/vim text editor.

Another way to search through events is using a date and time. When using this command, if date is omitted, the date for today is used. If the time parameter is omitted, the current time is used.
ausearch –ts today –k password-file
ausearch –ts 3/12/10 –k password-file

If the administrator needs to search for an event that matches an executable name, he should use "-x" parameter. For example, use "rm" command to find out who accessed /etc/passwd file:
ausearch –ts today –k password-file –x rm
ausearch –ts 3/12/10 –k password-file rm

Another situation that may rise is that the administrator needs to search for an event using a user name. For example, find out if user "mrcorrect", with unique identifier 506 tried to open /etc/passwd file:
ausearch –ts today –k password-file –x rm –ui 506
ausearch –k password-file –ui 506

5. MICROSOFT WINDOWS AND LINUX SECURITY COMPARISON

I believe the reason why Windows is subject to the most attacks is simply because it is the widest spread operating system. The fact of being the widest spread, alone, makes Windows a more attractive and a richer target for malware developers. Linux is also viewed as a system which derives its security from the design philosophy of UNIX.

The security researchers believe that "Windows monoculture" contributes to levels of malware exposure that are not proportionate. This means, that because Windows operating systems are tightly binary-compatible, a single attack to the system can affect a large number of them; this is also known as "cascade failure". This is in contrast with Linux operating system, which is more loosely coupled with source compatibility and different selections of software. This means that if the software is equally with bugs, the chance of one single bug affecting all of the Linux operating systems is reduced.

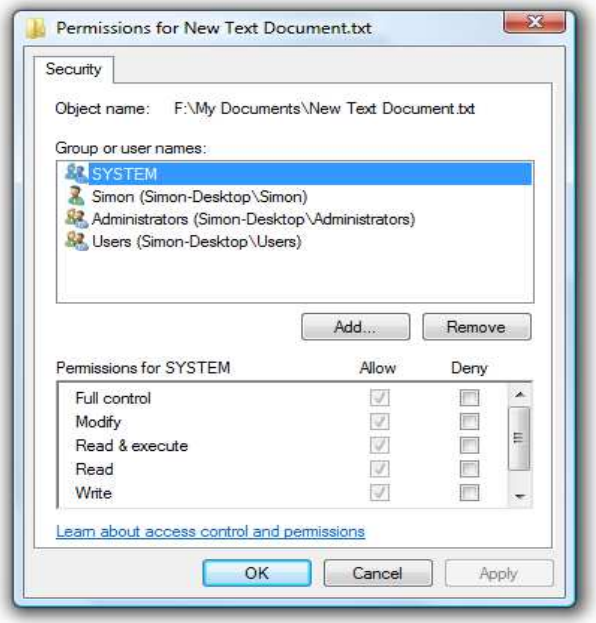

Figure 5. File System Permissions setting in Microsoft Windows operating system

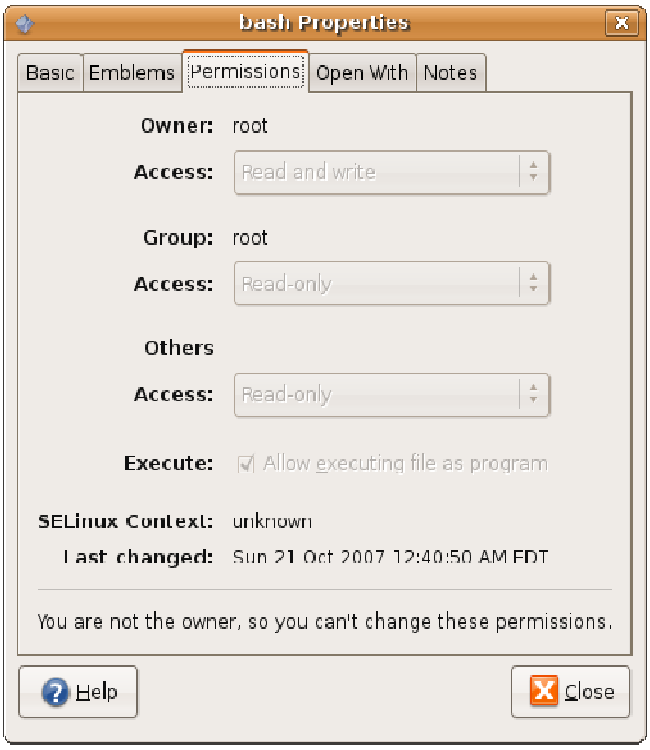

Figure 6. Linux version of file system permission setting called "Bash properties"

Criteria	Microsoft Windows	Linux
Malware	In [11], it is believe that over two million malware software target Windows operating system. Once malicious software is installed on a Windows operating system, it can, sometimes, be extremely difficult to locate and remove.	In [9], it is believed that over 800 Linux malware applications have been discovered.
Open vs. Close	A disadvantage of using Microsoft Windows is that it is a closed operating system, which means that only Microsoft employees has the source and only they can fix the security bugs.	Linux is an opened operating system and claims it is more secure because of the great number of people evaluating every release and working on bugs to make the system even more secure.
Response speed to security issues	Closed systems usually offer a great response speed for bugs and vulnerabilities. However, if there are critical bugs, the fixes are released only once a month.	In Linux, bugs are fixed a day after it was reported. Sometimes, they are fixed even within hours.
User accounts	In Windows there are login sessions, which provide standard user permissions	In Linux, there is typically a simple user account. At the installation of Linux it is

	for the logged user and prevent the user form accessing malicious software by displaying a dialog box. If the user has administrator privileges, than he only needs to press the ok button in the dialog box, but if he has normal user privileges he needs to enter the administrator credentials to access the application.	created an administrator user called "root" and at least another simple user account. If the logged user needs to elevate their privileges temporary they need to access "sudo" or "su" commands. These practices can be very dangerous as any error can bring serious damage to the system.
File permissions	Versions newer than Windows NT, support NTFS file system format which gives the opportunity to set permissions using Access Control Lists. Files System Permissions setting for Microsoft Windows operating system can be seen in Figure 5.	Linux offers its traditional user; group and other approach to setting file system permissions. On some file systems this approach can be extended by using Access Control Lists. Bash properties setting for Linux operating System can be seen in Figure 6.

Table 2 Microsoft Windows vs. Linux security comparison

In Table 2 there are the main key differences in security concepts between Microsoft Windows and Linux operating systems.

6. CONCLUSIONS

I have seen that the security of client operating system has at least the same importance as that of a server computer as they are the most targeted ones and they release the most attacks targeting both servers and clients systems.

Microsoft Windows security audit can be accomplished by using Local Security policies tool that can log successful or failed attempts for the configured list of events. Over the time, Windows operating system has improvement its auditing abilities evolving from nine categories of auditing events that can be monitored to 53 found in the Windows Vista and Windows 7.

Viewing audit reports in Microsoft is as simple as accessing Event Viewer application from administrative panel.

On the other hand, when using Linux operating system, you have to install some packages depending on the version and the distribution used. Using these packages, there are lists of terminal commands that need to be run in order to accomplish the desired audit procedure.

Queries and reports based on the audit log can also be done by using specific tools from the package, for querying you may use "ausearch" and for reporting "aureport".

When comparing the security of the two operating systems based on key security elements, I saw that there is no obvious winner when it comes to security. Linux seems to be the one with the most advantages due to the fact that it is an open source operating system and it follows the Linux "law", which states that Linux is more secure because any user can review its source code and contribute to fixing bugs.

With Linux having the advantage of being open-source the situation balances because Microsoft Windows offers better security for account based access using its proprietary user access level control. It also offers a better file system permission security, using the NTFS file system along with Access Control Lists.

REFERENCES

[1] D. Challet and D. Yann, Microscopic model of software bug dynamics: closed source versus open source, International Journal of Reliability, Quality and Safety Engineering, 2005

[2] F. Gallegos and S. Senft, Technology Control and Audit (2nd ed.), Auerbach Publications, 2004

[3] R. Goodman, Technology and strategy: conceptual models and diagnostics, Oxford University Press US, 1994

[4] T. Holwerda, Ballmer: Linux Bigger Competitor than Apple, http://www.osnews.com/story/21035/Ballmer_Linux_Bigger_Competitor_than_Apple, 2009

[5] M. Kalkuhl, Malware beyond Vista and XP, http://www.securelist.com/en/analysis?pubid=204792070, 2009

[6] D. Melber, Auditing Security and Controls of Windows® Server 2000 and Windows® Server 2003, The Institute of Internal Auditors Research Foundation, 2005

[7] R. Moeller, IT Audit, Control, and Security (Wiley Corporate F&A), Wiley, 2010

[8] Novell, OpenXDAS, http://openxdas.sourceforge.net/, 2009

[9] L. Poettering, A Guide Through The Linux Sound API Jungle, 0pointer.de, 2004

[10] S. Sayan, Auditing OS and Database Controls, http://www.isaca.org/Journal/Past-Issues/2003/Volume-3/Pages/Auditing-OS-and-Database-Controls.aspx, 2003

[11] F. Schießl, Zwei Jahre freie Software in München, 2008

[12] R. Winkler, Advanced Security Auditing in Windows 7 and Windows Server 2008 R2, http://social.technet.microsoft.com/wiki/contents/articles/advanced-security-auditing-in-windows-7-and-windows-server-2008-r2.aspx, 2010

[13] http://support.microsoft.com/kb/300549, How to enable and apply security auditing in Windows 2000, 2006

[14] http://www.addictivetips.com/windows-tips/windows-7-what-is-account-auditing-and-how-to-enable-it/, Windows 7: What is Account Auditing And How To Enable It, 2010

[15] http://www.niiconsulting.com/innovation/LinuxSecurity.ppt, Linux Security, 2008