Network and information security
Research Report

Group Project 1

Prepared by: GROUP 3

Preparation for Group Project 1 of Network and information security at Southeast University

Lecturer: Yong Jianming

10th December 2019

Summary

This report discusses how a computer's log files contribute to network and information security. we choose two different computers that one runs windows system and the other runs Mac OS system to analyze the log files' difference between two platforms.

Key findings include:

- Tables about the locations, types and functions of the log files in two platforms.
- Comparison of two different log file systems and some findings about their respective advantages and disadvantages.
- Explain how the log files can contribute to network and information security.
- A brief journal to record our sub-group activities, major events and each individual's contribution towards this project.

The report has been prepared for submission as Group Project 1 for Network and information security at Southeast University.

TABLE OF CONTENTS

1 Introduction

Log files record the necessary and valuable information for IT resource-related activities such as servers, workstations, firewalls, and application software, which are important for system monitoring, querying, reporting, and security audits. The records in the log files can provide the following uses: monitoring system resources, auditing user behavior, reporting suspicious behavior, determining the scope of intrusion, helping to recover the system, generating investigative reports, and providing a source of evidence to combat computer crime.

This report will shows that how different the log files work on two different log files systems.

1.1 Methodology

First we choose the Windows system and Mac OS system, then we divided into five sub-groups:
Sub-group 1 is going to organize the locations, types and functions of the log files on two different platforms.
Sub-group 2 is arranged to analyze the difference between the two log file systems and make a conclusion about their respective advantages and disadvantages.
Sub-group 3 do further research to find how the log file contribute to our network and information security.
Sub-group 4 will record everybody's contributions towards the project.
The last is planned to give the lecture. Also he needs to prepare 20 PPT slides.

If there are still some thing we can't understand, we choose to google it.

1.2 Scope of the report

We choose the log files in the Windows and Mac OS system with a time period between October and November in 2019. We do some researches on the types and function of the log files, also we compare the differences between the two log file systems in order to get more about how log files contribute to our system.

2. Findings

2.1 Types, Location and Function of the log files

According to what we learn, there are ten types of log files in Windows system.They are called System, Setup, Application, Security, Forwarded Events, HardwareEvents, Internet Explorer, Key Management Service, Windows PowerShell and IIS. Their locations and functions are shown in detail in the following table.

Table 1: Windows system

Log file type	Location	Function
System	C:\Windows\System32\winevt\Logs\System.evtx	Record system process, device disk activity and more. Including the device driver’s failure to start or stop normally, hardware failure, duplicate IP address, system start, stop and pause.
Setup	C:\Windows\System32\winevt\Logs\Setup.evtx	Record all actions that take place during installation
Application	C:\Windows\System32\winevt\Logs\Application.evtx	Record events about the application installed by the operating system., including errors, warnings and any information that an application needs to report and application developers can decide which information to log.
Security	C:\Windows\System32\winevt\Logs\Security.evtx	Record events about security, such as user permission changes, login and logout, file and folder access, printing.
Forwarded Events	C:\Windows\System32\winevt\Logs\Forwarded Events.evtx	Forbidden
HardwareEvents	C:\Windows\System32\winevt\Logs\HardwareEvents.evtx	Record events about hardware

Internet Explorer	C:\Windows\System32\winevt\Logs\Internet Explorer.evtx	Record log information of the IE browser application, which is not enabled by default and needs to be configured through Group Policy.
Key Management Service	C:\Windows\System32\winevt\Logs\Key Management Service.evtx	Record information about key actions.
Windows PowerShell	C:\Windows\System32\winevt\Logs\Windows PowerShell.evtx	Record log information for the PowerShell application that comes with Windows.
IIS	C:\Windows\System32\LogFiles	Record information including user ip, web address,, visiting time, visiting state and so on each time opening a website

As for the other system, Mac system, there are also ten types of log files in it, which are called Installer, Power Management, Copy CD, kernel, File system repair, User system repair, System, IORegistry, NVRAM, Wi-Fi. Moreover, their locations and functions of each of them are listed in the following table2.

Table2: Mac system.

Log file type	Location	Function
Installer	/var/log/install.log	Record program installation information
Power management	/usr/bin/pmset -g log	Record information about battery status
Copy CD	/Users/liuguiling/Library/logs/DiscRecording.log	Record CD burn information
kernel	/var/log/asl	Store kernel-generated logs
File system repair	/var/log/fsck_hfs.log	all file’s information
User system repair	/Users/liuguiling/Library/logs/fsck_hfs.log	record the system user login and exit the system related information, including user name, login terminal, login time, source host, the process operation in use, etc

System	/var/log/asl	Record information about hardware, software, and system problems in the system, as well as monitor events that occur in the system
IORegistry	/usr/sbin/ioreg -lxw550	Record the IO stream
NVRAM	/usr/sbin/nvram -xp	Record the basic information such as the model and parameters of the equipment put in the factory
Wi-Fi	/var/log/wifi.log	Record the information of each WiFi connection

2.2 Comparison of two different log file systems

Mac file system and Windows file system have three points of similarities.First of all, both Mac OS and Windows system have log files for program installation and set up. Moreover, Mac OS logs contain information about hardware, software, system issues, and monitor events, and the Windows system divides this kind of log files into hardware logs and the system logs. The MAC OS focuses on recording all relevant information, while Windows system focuses on recording errors. At last, Mac OS divides security-related logs into two modules: file system repair and user system repair, which record all file information and user log-in and logout information respectively. The Windows security log covers all aspects of security, including user license changes, user login and logout, access to files and folders, and printing.

However, they both have their own advantages and disadvantages, which will be shown as follows. First we will show the advantages and disadvantages of Mac. Then we will talk about Windows file system.

There exist four advantages in Mac file system. First of all, MAC OS has logs for basis parterns, such as System、File system repair、Installer、User system repair and detailed records of hardware and configuration, including system logs for Power management, Copy CD, kernel, Wi-Fi and IORegistry. Secondly, All log files for MAC OS are respectively stored in three different paths. The first section holds the Wi-Fi, kernel, File system repair, System and Installer log files under the /var/log path. The first section holds User system repair and Copy CD log files under the /Users/liuguiling/Library/logs path. The first section holds Power management, IORegistry and NVRAM log files under the /usr/bin path. The classification is clear and easy to manage.Moreover, MAC OS log files can be used to restore the file system to a known consistent state. After the server is restarted, the Mac OS simply performs the most recent transaction in the log to update the system to the latest state and continue the operations interrupted during the failure.Lastly, The MAC OS system has a special tool for viewing log files. After logging in as an administrator, you can view and search log files, which improves the convenience and security to some extent.

Compared with Windows system, MAC OS has relatively less management of application and network usage. For example, Windows system has but MAC OS system

does not record: Application, IE, Key Management Services, Windows PowerShell and IIS log files.Mac

Next, we will talk about Windows file system. Firstly, the information covered by the Windows event log files is relatively comprehensive and classified clearly. Moreover, in contrast to the Mac OS, there is a dedicated logging module for logging specific application information in Windows file system. Windows log file system provides a module to record application-related event logs. Windows log file system design the corresponding log file modules for software and tools specific to Windows. Thirdly, Windows system comes with a log analysis tool called event viewer, clearly dividing log files into various types, making it convenient for users to view and manage relevant log information. On Windows system, the event viewer filters, sorts, and extracts logs into files for users to analyze fault and security information. The event viewer divides logs into two parts: the Windows logs and the application and service logs. The Windows logs include the information about log system, security and application. And the application and service logs cover the information of Microsoft, Microsoft Office Alerts, Windows PowerShell and Internet Explorer. Lastly, Windows event log files are stored in the evtx format for unified management. EVTX event log files can be exported as EVTX, XML, TXT, and CSV files using the event viewer tool.

There certainly are disadvantages in Windows file system. Compared to Mac OS, it lacks log information on power management, CD, kernel, IO, NVRAM and Wi-Fi. Event log files (evtx) are binary formats that not only require proprietary tools or programs to read and process them, but their long-term storage presents many challenges for enterprise users.At last, Windows event log files have poor security, vulnerable to hacker attacks.

2.3 How the log files contribute to network and information security

The log file records every detail of the operation of the system and its various services. By continuously monitoring the log file entries, intrusions can be detected, helping us understand and avoid some disasters .

In network communication, analysis of various log in events can effectively find evidence of hackers trying to log in and intrusion of information. At the same time, if the system finds abnormal log in log information, it can prevent in time and notify users to pay attention to security.

If a hacker hacks, it may modify the user's security protection measures and operate on the file information. These operations will leave a record in the system log. By analyzing these log files, users can learn which security measures have been modified, and which information has been stolen. It helps provide available data for handling incident.

Log files are also important in processing system failures caused by force majeure. On the one hand, the log file records what operations the system has performed to understand what caused the system failure; on the other hand, the sudden failure of the system may cause abnormal information and data. The log file can effectively restore the information and data to the last normal state, which prevents the loss of overall information and data.

The maintenance personnel can quickly locate the faults and check the causes of them to let network perform well through analyzing log files. At the same time, log files provide the trace to track the attacker to strengthen the network security level and improve the network security performance

2.4 Journal recording the work members do

11.2
Discuss project planning and identify computers running two different platforms, Mac and Windows. Searched a lot of information on the Internet and learned more about log files. Complete the division of labor as follows:
姜子玥，刘桂伶： task2 and task6
丁婧伊，刘雪珂： task3
魏旭凯，袁佳怡： task4
张晨旭： task5
李雨峤： ppt preparation and speech

11.25
The working arrangement of task3 was planned, and in 12.1, the forms including the comparison and comparison of the two log file systems, the word document, and the advantages and disadvantages of the two log file systems were analyzed (one Chinese and one English).

12.2
Completed task2's work report and screened the thesis template, summarized the problems encountered in the first half of the project, and tried to avoid and further improve the quality of the entire project in the next task.

12.3
Discuss the completion progress of task4, discuss the general structure and focus of the paper, improve the efficiency of the tasks of the remaining team members, and the project enters the final sprint stage.

12.5
Completed task4, further researched the log files of mac and windows, and the thesis is also under intense completion and enrichment.

12.6
Prepared the summary and integration, determined the completion time of the paper, and the group discussed the project together. Finally, the integration of the thesis and various tasks was completed in 12.8.

3. Conclusion

The two log file systems we research have some log files in common. However, the Mac OS classification of log files focuses more on hardware and configuration (including power, CD, wi-fi, etc.), while Windows system focuses more on applications and networking (including the use of Windows PowerShell, IE, IIS, etc.).

Based on the above findings, the two log file systems have their own ways to protect themselves from attacking. Therefore, we have understood more deeply on the network and information security.

4. Recommendation

The log files are of great significance to our system. As a future IT worker, we would better perfect ourselves in resolving the problems in systems with the records in the log files. For example, you can use the log files to search for your historical operations. So when facing with a catastrophic problem, you can use the log file to retrieve information and discover the problem.

5. Reference List

https://support.apple.com/zh-cn/HT204435

https://support.apple.com/zh-cn/guide/console/cnslbf30b61a/mac

https://blog.csdn.net/qq_27446553/article/details/80906390#commentBox 作者：TomKing

https://www.secpulse.com/archives/110283.html 作者：Lemon

https://blog.fox-it.com/2017/12/08/detection-and-recovery-of-nsas-covered-up-tracks/ 作者：Wouter Jansen

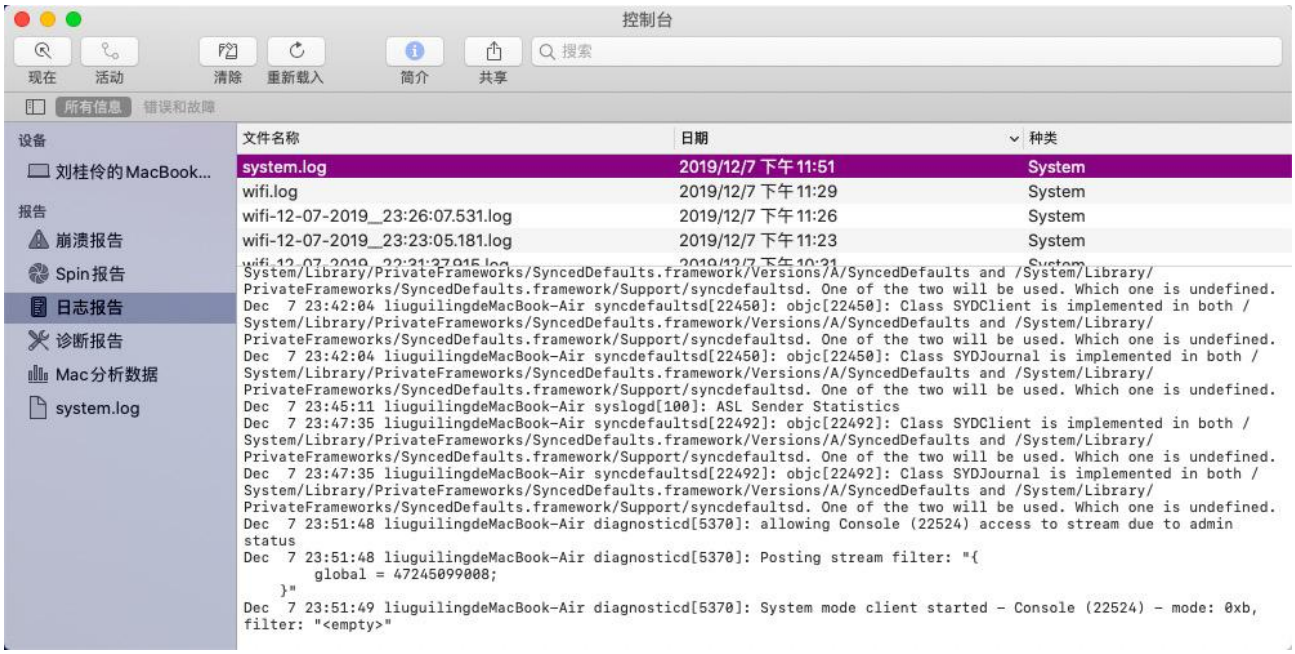
https://www.ixueshu.com/document/0487c9602a1a9314030c50248281395e318947a18e7f9386.html 作者：丁谊

https://www.ixueshu.com/document/28ef82255642a856.html 作者：张俊林

https://wenku.baidu.com/view/c2ed2adbad51f01dc281f18b.html

6. Appendix

Appendix A: Log file viewer in Mac OS



Appendix B: Log file viewer in Windows