

Log in Operating Systems

Group 6

1 TASK ANALYSIS

1.1 Two operating systems

We choose Windows and Ubuntu as our experiment subjects. (Windows 10 1903 update. Ubuntu 18.04.3 LTS)

1.2 Log files analysis

Log is an important part of operating systems, Windows and Ubuntu systems have different system log structures. We want to pick out the structure of Windows and Ubuntu operating systems' logs in this part, and tag the use and lifeline of each log (When logs are produced. Why logs are produced.) We also want to match logs to their producers.

2 INTRODUCTION

2.1 Method introduction


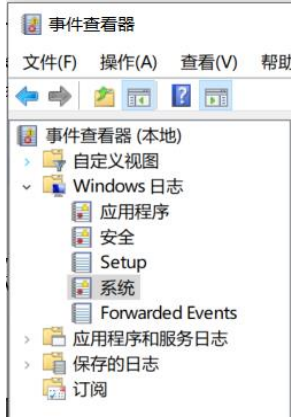
In this subsection, we plan to search on Internet for the structure of Ubuntu and Windows's log file systems (How to store logs). Then for each folder, we find the time of generation, generated event and producer for each log in the folder. We mainly analyze the security of users' actions and the failures of system core related to logs.

3 MEASUREMENT RESULTS AND ANALYSIS

3.1 Motivation

In this section, we generally introduce how we organize Ubuntu system log files. We use the system's classification method, and the results are shown in Fig. 1. We mainly analyze logs related to security and system.

Fig. 1. Classification Method

| | |
|--|--|
|  <p>Important</p> <p>All</p> <p>Applications</p> <p>System</p> <p>Security</p> <p>Hardware</p> |  <p>事件查看器</p> <p>文件(F) 操作(A) 查看(V) 帮助</p> <p>事件查看器 (本地)</p> <ul style="list-style-type: none"> 自定义视图 Windows 日志 <ul style="list-style-type: none"> 应用程序 安全 Setup 系统 Forwarded Events 应用程序和服务日志 保存的日志 订阅 |
| Ubuntu system | Windows system |

3.2 Methodology

We find that Ubuntu system log files are all placed under the folder: `/var/log`. For each log file, detailed information is shown in Table.1.

Table 1. Log Files

| Name | Briefly Information | Remarks |
|------------------|---|---------|
| alternatives.log | Update & system replace | |
| apport.log | Application crash | |
| apt/ | Install & uninstall application | folders |
| auth.log | Login check | |
| boot.log | System boots | |
| btmpt | Failure record | |
| Consolekit | Console information record | |
| cpus | Printed information | |
| dist-upgrade | Update information using dist-upgrade | |
| dmesg | Kernel ringbuffer, show hardware information on screen when poweron | |
| dpkg.log | Install & uninstall dpkg application package | |
| faillog | User login failure and wrong commands | |
| fontconfig.log | Typeface related logs | |
| kern.log | Logs produced by system kernel, can help when customize system kernel | |
| lastlog | Recent information of all users.(Not ASCII | |

| | | |
|----------|--|--|
| | type, use lastlog command to read) | |
| mail | Mail system server addition logs | |
| mail.err | Mail system server error logs | |
| wtmp | Login information. Can be used to find who is connecting with system & which file or information have it checked | |

To analyze Windows log file system, firstly we locate windows system's log files in the location: %SystemRoot%\System32\winevt\Logs. All log files lay under the folder without any optical structure. Then, we use windows-event-viewer for a better organization of log files structure. The brief structure is shown in Table.2.

Table 2. Brief Structure

| Application & Security | | | | |
|------------------------|------|--------|----|------------|
| Key word | Time | Source | ID | Event kind |
| System | | | | |
| Level | Time | Source | ID | Event kind |

3.3 Results

For Ubuntu system, we choose two logs and analyze their detailed information. First, we briefly arrange the structure of *auth.log* and *alternatives.log*. The results are shown in Table.3.

Table 3. Ubuntu Log Files Details

| auto.log | | | |
|-----------------|------------|-------------|---|
| Time | IP Address | Protocol | Description |
| Nov 22 06:26:11 | localhost | sshd[13118] | Failed password for root from 49.51.153.55 port 54128 ssh2 |
| Nov 22 06:28:01 | localhost | CRON[13202] | pam_unix(cron:session): session opened for user root by (uid=0) |

| alternatives.log | | |
|------------------|------|-----------|
| Activities | Time | Operation |

| | | |
|-------------------------|------------------------|---|
| update- alternatives | 2019-11-04 16:11:23 | run with --install /etc/mysql/my.cnf my.cnf /etc/mysql/mysql.cnf 200 |
|-------------------------|------------------------|---|

We find that, two log files both record timestamp in their attributes. This situation is common in logs, because time is a strong proof when back tracing an event (attack or accident). User's IP addresses with protocol and port are recorded in description of *auto.log* to identify a login action. APT command and influenced folders are recorded in *alternative.log* to record an update or upgrade operation.

Then, for Windows system we make a brief conclusion of security and system logs' information details. The results are shown in Table.4.

Table 4. Windows Log Files Details

| Security | | |
|--|------|--|
| Source | ID | Description |
| Microsoft Windows security auditing. | 4624 | Successfully login account |
| | 4634 | Successfully logout |
| | 4672 | Distribute special authority for new login |
| | 4797 | Try to find blank password account |
| | 4798 | Enumerated local group user account |
| | 4907 | Object check rules verification |
| | 5379 | Credentials manager |
| | 5382 | Vault credentials |

| System | | |
|---------------------------|----|--|
| Source | ID | Description |
| Killer Network Service | 0 | Service started/resumed |
| Kernel-General | 1 | System time change |
| Kernel-Power | 42 | System is entering sleep state Cause: Application API |

| | | |
|--|-----|----------------------------------|
| | 105 | Power change |
| Windows-Update-Client | 43 | Update activated |
| | 44 | Windows update begin to download |
| Kernel-Processor-Power (Microsoft-Windows-Kernel-Processor-Power) | 55 | Power limitations setting |

3.4 The comparison of log system in Windows and Ubuntu Systems

Table 5. Comparison of Log System in Windows and Ubuntu Systems

| Aspects | Windows System | Ubuntu System |
|-----------------|---|--|
| Location | <i>%SystemRoot%\System32\winevt\Logs</i> | <i>/var/log</i> |
| Types | All versions of Windows System contain the same classification with following types: systems, security, applications, setup | Log file types are more detailed, according to different application or activity classification, such as system kernel, mail, network, timestamp, etc. But not all Ubuntu systems include these types. |
| Priority | No priorities between each log | Priorities From 'emergency' to 'no priority' (not logging any log messages) |
| logging service | Common Log File System (CLFS) | Syslog. Syslog can save logs to different files depending on the type and priority of the logs |
| Access method | Event Viewer | Opening the log files for viewing. Some log files can be accessed from terminal directly |

3.5 The advantages and disadvantages of log systems in Windows and Ubuntu systems

Windows:

Advantages:

1. The log type is relatively uniform. The log types are same on different versions of the system, which is easy to manage and archive.
2. Logs can be viewed through the *eventvwr graphical interface*, which automatically integrates all log files for easily operation.

Disadvantages:

1. log types are few and rough, not convenient for carefully reviewing log information.
2. The log has no priority and is not convenient for troubleshooting.

Ubuntu:

Advantages:

1. There are many log types to help the information searching.
2. The logs are not only classified by type, but also by priority, which can help the administrator to find more urgent and important problems.

Disadvantages:

1. Log types are complex and complicated.
2. Although some terminal commands can check the log information directly, most of the log files checking needs to jump to the directory where the logs are located, which is inconvenient to operate.

3.6 Discussion

With the advent of the Internet age, there are more and more types of logs in the network. In the network age, whoever masters the data will master the initiative. In addition to the security operation and maintenance, the log data in the network information security can also be used to counter the information network attacks and situational display.

We find that in Ubuntu system, root level users can easily change containments in log files (Even *auth.log* and other *sensitive logs*). This finding shows root authority can cause great damage to the system.

4 CONCLUSION

Ubuntu has prefect authority management mechanism, but it opens too many permissions to root users. System manager in root can work efficiently meanwhile manager may cause irreversible damage to system accidentally.

4.1 THE ROLE OF THE LOG

In this section, we'll discuss the conventional role of the log in network and information security.

The log data in information security is mainly obtained from the operation of network infrastructure such as network devices, security devices, servers, middleware, etc., which reflects the traces of network operation and the clues of user operations. These data are more used to help network security operation and maintenance, security

management, to detect network security threats, notify operation and maintenance personnel when security incidents occur, assist in tracking traceability after security incidents, and help users to grasp the overall security posture of the network.

After the log audit system collects the logs of various log sources, the logs are parsed according to the log source type. This process is also called log formatting. After the log is formatted and stored, if the security event occurs, the log auditing system can notify the operation and maintenance personnel of the alarm by SMS, email, sound and light, etc., so that the operation and maintenance personnel can handle the security incident in time. At the same time, the system can perform statistical analysis on various security logs and security events through various pre-made reports, so that operation and maintenance personnel and management personnel can master the network security status. This can play a very important role in network operation and maintenance, and can meet the security needs of enterprises.

4.2 Comparison

The Windows System log contains the following types: systems, security, applications, setup, and Ubuntu System log contains information entry, mistake or failure information from the corresponding log records. The Ubuntu System log have the priorities from 'emergency' to 'no priority' while the Windows System log has no priorities. Windows logs can be viewed through the event log viewer, while Ubuntu logs can be viewed through the logs view tool.