**1 TASK ANALYSIS**

* 1. **Two operating system**

We choose Windows and Ubuntu as our experiment subjects.(Windows10 1903 update. Ubuntu 18.04.3LTS)

**1.2 Log files analysis**

Log is an important part of operating system, Windows and Ubuntu system have different system log structures. We want to pick out the structure of Windows and Ubuntu operating system’s log in this part, and tag the use and lifeline of each logs(When are they 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 structure of Ubuntu and Windows’s log file system(How to store). Then for each folders, find the production time, production event and producer for each logs in the folder, We mainly analysis user action security and system core failure related 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, result is shown in Fig.1.We mainly analysis security and system related logs.

Fig. 1. Classification Method

|  |  |
| --- | --- |
| Ubuntu system | Windows system |

**3.2 Literature Review(If you read some references.)**

**3.3 Methodology(How do you do the task, in detail)**

We find that ubuntu system log file are all place under folder /var/log. For each log files detail introduction are 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 |
| btmp | Failure record |
| Consolekit | Console information record |
| cpus | Printed information |
| dist-upgrade | Updata 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 analysis Windows log file system, we first find windows system’s log files in the location %SystemRoot%System32/winevt/Logs. All log files are lay under the folder without any optical structure. Then, we use windows event viewer for a better organization of log file structure. The brief structure are shown in Table.2.

Table 2. Brief structure

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

**3.4 Result(Show result in detail. Explanation is required)**

For Ubuntu system we choose two logs and analysis their detail information. First, we briefly arrange the struct of auth.log and alternatives.log. The result are shown in Table.3.

Table 3. Ubuntu Log Files Detail

|  |  |  |  |
| --- | --- | --- | --- |
| **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 prove when back tracing an event (Attack or accident). User IP address with protocol and port are recorded in description of auto.log to identify a login action. APT command and influenced folder are recorded in alternative.log to record a update or upgrade operation.

Then, for Windows system we make a brief conclusion of security and system log information detail. The result are shown in Table.4.

Table 4. Windows Log Files Detail

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

**3.5 Discussion(Maybe some issues are found, report the issues and try to find reason)**

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 user can easily change containments in log files(Even auth.log and other sensitive logs). This finding shows root authority can cause great damage to system.

**4 CONCLUSION(What you learn from this experiment. What’s your felling.)**

Ubuntu has prefect authority management mechanism, but it open to many permission to root user. 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 It is 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.

These logs record the path that the O&M personnel, the general end user, the external user access when using the system, the visitor IP, the user name of the login system, and the submission parameters. When an attack occurs, the attacker’s attack time, attack mode, attack IP, and so on can be recorded. Even if the network security device does not match the attack, when the attacker attacks, the device that the attacker enters the network records the attacker’s access path, operation mode, and submission parameters. Generally, after an attacker completes an access or an attack, the access record left by the attacker is deleted. Therefore, keeping the logs of various devices in the network is a very necessary means for discovering the attack and performing traceback after the event to solve the problem.

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.