**1 TASK 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 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**

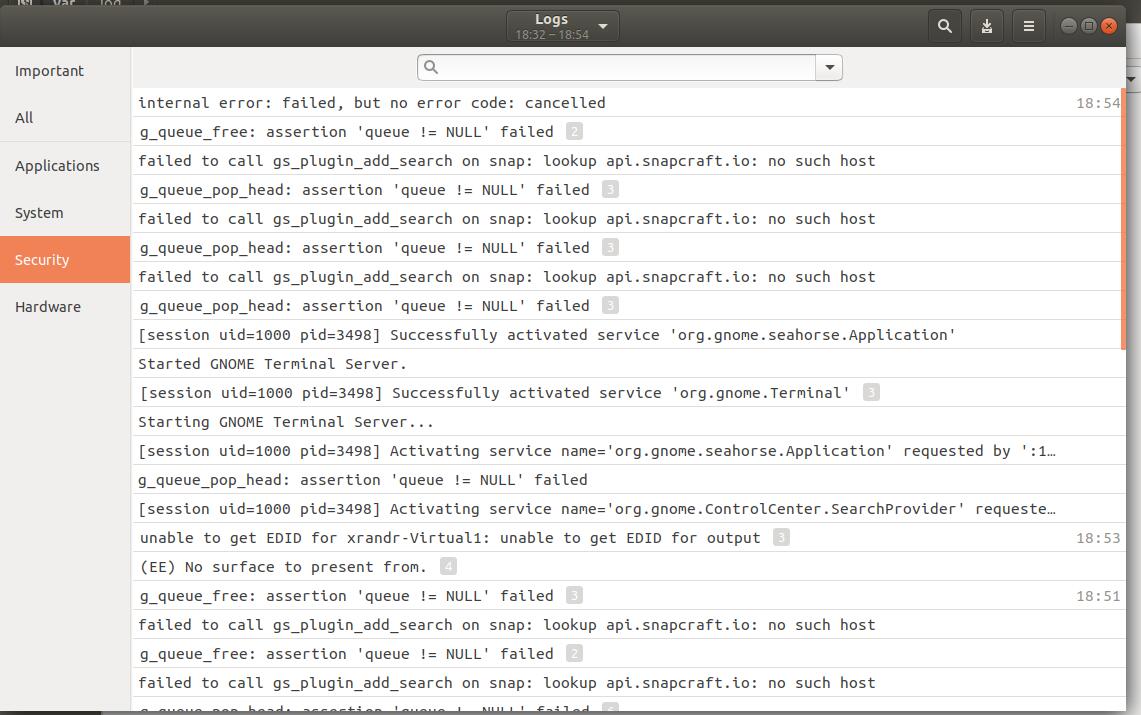
The experience environment we choose is Ubuntu18.04LTS. We plan to search on internet for structure of log file system(How to store). Then for each folders, find the production time, production event and producer for each logs in the folder, We mainly analysis user action security and system core failure 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



**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 |  |

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

We choose three logs and analysis their detail information. First, we briefly arrange the struct of auth.log& alternatives.log& mail. The result are shown in Table.2.

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

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.

**3.6 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.