系統程式 HW5

410410060 資工二 林柔均

編寫程式

加上檔案類型

```
void initFileTypoe() {
    for (int i=0; i< 99; i++) {
        filetype[i] = -1;
    }
    /*同學自己補下去*/
    fileSymbol[DT_BLK]='b';
    fileSymbol[DT_CHR]='c';
    fileSymbol[DT_DIR]='d';
    fileSymbol[DT_FIFO]='f';
    fileSymbol[DT_LNK]='l';
    fileSymbol[DT_REG]='-';
    fileSymbol[DT_SOCK]='s';
    fileSymbol[DT_UNKNOWN]='u';
}
```

加上 fileNum 變數紀錄檔案的數量

```
*/
long myCountDir(char* path) {
    long size = 0;
    //打開該目錄
    DIR* dirp = opendir(path);
    //讀取該目錄的第一個「物件」
    struct dirent* ent = readdir(dirp
    while (ent != NULL) {
        fileNum++;
        //『這個目錄』及『上一層目錄』
        if (strcmp(ent->d_name, "." )
            ent = readdir(dirp);
            continue;
        }
```

執行程式

需要將檔案變成 super user, 加入 set user id bit

- `sudo chown root preBirthday`
- `sudo chmod +s preBirthday`

```
all: preBirthday
preBirthday: preBirthday.c
    gcc preBirthday.c -o preBirthday
    sudo chown root preBirthday
    sudo chmod +s preBirthday
clean:
    rm preBirthday
```

第一次執行出現 segmentation fault

```
 ~/De/homework/SystemProgramming/hw5 ❯ ./preBirthday /
授課老師（羅習五）的生日是: 1990/04/10
zsh: segmentation fault (core dumped)  ./preBirthday /
```

Google 後發現要將 `/proc/sys/fs/suid_dumpable` 裡的值改成 2

```
 ~/De/homework/SystemProgramming/hw5 ❯ cat /proc/sys/fs/suid_dumpable
2
```

更改後執行就沒問題了

```
 ~/De/homework/SystemProgramming/hw5 ❯ ./preBirthday /
授課老師（羅習五）的生日是: 1990/04/10
總檔案大小: 39535314948 bytes
檔案種類: fcdb-ls
檔案數量: 1438627
```

檔案類型的意義

- `b` : 區塊設備檔，可以隨機在硬碟不同區塊讀寫儲存的資料
- `c` : 字元設備檔，序列埠週邊設備(鍵盤、滑鼠)
- `d` : 目錄檔案
- `f` : pipe 管線檔案(FIFO)，類似於 queue，將資量順序放入取出
- `l` : 連結檔案，可簡化路徑
- `-` : 一般檔案

- `s` : 資料接口檔(sockets)，讓 clien,server 端進行資料的溝通
- `U` : 無法辨別的檔案

加註: suid_dumpable 的參數

- 1- A regular user can trigger a coredump with /proc/$PID/stat as root:root simply by doing chmod u-r
- 2- The root-owned coredump will then be written in the CWD, which in the PoC is /etc/logrotate.d
- 3- logrotate will gladly skip parts of the coredump it doesn't understand and will successfully run the parts it does

https://bugs.launchpad.net/ubuntu/+source/apport/+bug/1452239