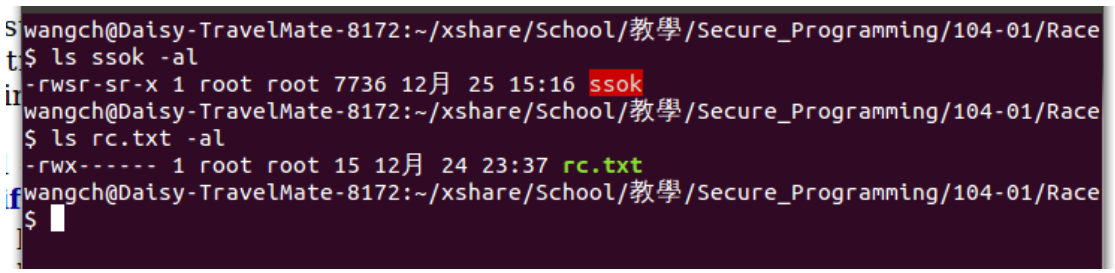
SetUID 補充說明

以下對於上課關於 setuid 的相關內容補充說明，利用執行 ssok 這隻程式來解說：

1. 下圖為 ssok 及 rc.txt 檔案資料。ssok 以設定 setuid 的權限，而 rc.txt 為僅有 root 的權限可讀取。且其 owner 為 root。



2. ssok.c 的程式如下：

```
#include <stdio.h>
#include <stdlib.h>
#include <fcntl.h>

int main(){

int fd, now_uid = getuid();
char name[30];
char str1[50];
uid_t ruid, euid, suid;

printf("<Initialization>\n");
printf("UID: %d \nGID: %d\n", now_uid, getgid());
getresuid(&ruid, &euid, &suid);
printf("%d, %d, %d\n", ruid, euid, suid);
system("/usr/bin/id");

printf("Please enter the filename: ");
  scanf("%s", name);
  fd = open(name, O_RDONLY);
     if (fd !=-1){
        printf("Open File OK (1) \n");
        read(fd, str1, 49);
        printf("File: %s", str1);
     }
     else
        printf("No permission! (1) \n");

  printf("%d\n", fd);
```

```
if (setuid(0))
{
printf("Setuid Error!");
return -1;
}
printf("<Get Root Permission>\n");
printf("UID: %d \nGID: %d\n", now_uid, getgid());
system("/usr/bin/id");
getresuid(&ruid, &euid, &suid);
printf("%d, %d, %d\n", ruid, euid, suid);

 fd = open(name, O_RDONLY);
    if (fd !=-1){
       printf("Open File OK (2)\n");
       read(fd, str1, 49);
       printf("File: %s", str1);
    }
    else
       printf("No permission! (2)\n");

 printf("%d\n", fd);

//drop root permission
printf("<Drop Root Permission>\n");
setuid(now_uid);
printf("UID: %d \nGID: %d\n", now_uid, getgid());
system("/usr/bin/id");
getresuid(&ruid, &euid, &suid);
printf("%d, %d, %d\n", ruid, euid, suid);

 fd = open(name, O_RDONLY);
    if (fd !=-1){
       printf("Open File OK (3)\n");
       read(fd, str1, 49);
       printf("File: %s", str1);
    }
    else
       printf("No permission! (3)\n");

 printf("%d\n", fd);

return 0;
}
```

3. 該程式有三部份：
   (1) （紅色）第一個部份是初始階段，假設執行該程式的使用者為 wangch (1000)。由於 ssok 程式為可設定 setuid 權限，而 rc.txt 的 owner 為 root 所以，當開始執行時，此程序的 effective ID (euid) 會被設定為 root。

也就是 (ruid, euid, suid)= (1000, 0, 0) 這情形下 rc.txt 可被正常打開。

(2) （綠色）第二部份是執行 setuid(0) 則，會把該程序的 ruid, euid, suid 均設為 root (0)。這情形下 rc.txt 可被正常打開。

(3) （藍色）第三部份是執行 setuid(now_uid) 則會將該程序的 ruid, euid, suid 均設為 wangch (1000)，如此，則會 permanently drop root permission。也就是 root 權限將永移除。這情形下 rc.txt 將無權限開啟。