

408410007 鄭雅云

題目：

將 nice 複製到自己的目錄下，名為 nice_pro，必且讓 nice_pro 擁有提高優先權的能力。

(這個是測試，當 nice-pro-test 沒有 super-user 的權限或是提高優先權的權利，會出現權限不足的問題。)

```
ariel@ariel-vm:~/system-programming/ch08/408410007hw8$ cp /usr/bin/nice nice-pro-test
ariel@ariel-vm:~/system-programming/ch08/408410007hw8$ ./nice-pro-test -n -10 ls
./nice-pro-test: cannot set niceness: Permission denied
```

sudo setcap CAP_SYS_NICE+ep 給 nice-pro 有提高優先權的權利

/nice-pro-2 檔案 change owner 變到 root (root:root—用戶名：用戶組)

使用 chmod +s 會給 nice-pro2 所有 super-user 的權限

```
ariel@ariel-vm:~/system-programming/ch08/408410007hw8$ whereis nice
nice: /usr/bin/nice /usr/share/man/man1/nice.1.gz /usr/share/man/man2/nice.2.gz
ariel@ariel-vm:~/system-programming/ch08/408410007hw8$ cp /usr/bin/nice nice-pro
ariel@ariel-vm:~/system-programming/ch08/408410007hw8$ cp /usr/bin/nice nice-pro-2
ariel@ariel-vm:~/system-programming/ch08/408410007hw8$ sudo setcap CAP_SYS_NICE+ep ./nice-pro
[sudo] password for ariel:
ariel@ariel-vm:~/system-programming/ch08/408410007hw8$ sudo chown root:root ./nice-pro-2
ariel@ariel-vm:~/system-programming/ch08/408410007hw8$ sudo chmod +s ./nice-pro-2
ariel@ariel-vm:~/system-programming/ch08/408410007hw8$ nice -n -10 ls
nice: cannot set niceness: Permission denied
Nice-hw.c nice-pro nice-pro-2 nice-pro-test
ariel@ariel-vm:~/system-programming/ch08/408410007hw8$ ./nice-pro -n -10 ls
Nice-hw.c nice-pro nice-pro-2 nice-pro-test
ariel@ariel-vm:~/system-programming/ch08/408410007hw8$ ./nice-pro-2 -n -10 ls
Nice-hw.c nice-pro nice-pro-2 nice-pro-test
```

討論：使用 sudo setcap CAP_SYS_NICE+ep，只給“提高優先權的權利”為佳，另一個方法若駭進來便可控制整個根目錄。

1. 從 man capabilities 裡面隨便挑三個權限，並說明那三個權限是什麼樣的用途：

CAP_AUDIT_READ：允許通過 multicast netlink 讀取審計日誌。

CAP_AUDIT_WRITE：寫東西進入內核審計日誌。

CAP_BLOCK_SUSPEND：可以阻止系統休眠。

2. 想辦法量測『優先權高一等級的 task 比正常優先權的 task 速度快多少』？

加入程式碼：

```
#define _GNU_SOURCE /* See feature_test_macros(7) */
#include <sched.h>
```

...

cpu_set_t mask; //CPU 核的集合

CPU_ZERO(&mask); //清空一個集合

CPU_SET(1,&mask); //先做好參數設定，綁在第一顆處理器

```
sched_setaffinity(0, sizeof(mask), &mask); //設進程為0, 讓它運行在設定的CPU上。
```