

## Hw8 量測 nice 的效果

系級：資工二 學號：409410114 姓名：周述君

- Setcap : capabilities 用於分割 root 用戶的特權，將 root 的特權分割成不同的能力，CAP\_CHOWN 用來修改文件主人的權限

`./chown_super sujean /usr/bin/ls` : 更改 ls 的使用者為 sujean

`./chown_super root /usr/bin/ls` : 更改 ls 的使用者為 root

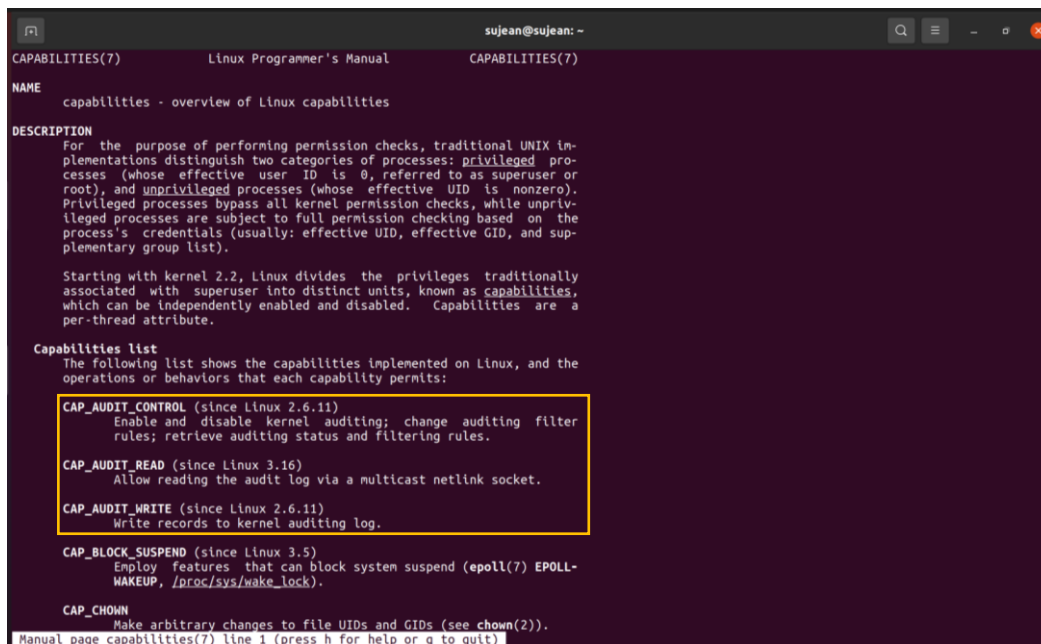
```
sujean@sujean:~$ ./chown_super sujean /usr/bin/ls
sujean@sujean:~$ ls -als /usr/bin/ls
140 -rwxr-xr-x 1 sujean root 142144 九  5 2019 /usr/bin/ls
sujean@sujean:~$ ./chown_super root /usr/bin/ls
sujean@sujean:~$ ls -als /usr/bin/ls
140 -rwxr-xr-x 1 root root 142144 九  5 2019 /usr/bin/ls
sujean@sujean:~$
```

- 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

```
sujean@sujean:~$ whereis nice
nice: /usr/bin/nice /usr/share/man/man2/nice.2.gz /usr/share/man/man1/nice.1.gz
sujean@sujean:~$ cp /usr/bin/nice nice-pro
sujean@sujean:~$ cp /usr/bin/nice nice-pro-2
sujean@sujean:~$ sudo setcap CAP_SYS_NICE+ep ./nice-pro
sujean@sujean:~$ sudo chown root:root ./nice-pro-2
sujean@sujean:~$ sudo chmod +s ./nice-pro-2
sujean@sujean:~$ nice -n -10 ls
nice: cannot set niceness: Permission denied
App      chown_super Documents Dropbox      glibc-2.31 Music  nice-pro-2 program-design snap  sp_mid Templates
busybox Desktop Downloads eclipse-workspace java-2021-12 nice-pro Pictures Public  sp  system-programming Videos
sujean@sujean:~$ ./nice-pro-2 -n -10 ls
App      chown_super Documents Dropbox      glibc-2.31 Music  nice-pro-2 program-design snap  sp_mid Templates
busybox Desktop Downloads eclipse-workspace java-2021-12 nice-pro Pictures Public  sp  system-programming Videos
sujean@sujean:~$
```

1. Nice 無法提升優先權 (只有 root 權限可以提升優先權)
2. Sudo setcap CAP\_SYS\_NICE+ep 只給 nice-pro 提高優先權的權利，如果 nice-pro 有安全性漏洞，則執行檔案被破解，駭客只拿到提升優先權的權限
3. 使用 chmod+s 會給 nice-pro-2 所有 super-user 權限，如果 nice-pro-2 有安全性漏洞，則執行檔案被破解，駭客就能拿到 super user 的權限

一、從 `mancapabilities` 裡面隨便挑三個權限，並說明那三個權限是什麼樣的用途（大致上就是英文翻譯成中文再加上一點點自己的理解）



```
sujean@sujean: ~
CAPABILITIES(7)      Linux Programmer's Manual      CAPABILITIES(7)

NAME
  capabilities - overview of Linux capabilities

DESCRIPTION
  For the purpose of performing permission checks, traditional UNIX im-
  plementations distinguish two categories of processes: privileged pro-
  cesses (whose effective user ID is 0, referred to as superuser or
  root), and unprivileged processes (whose effective UID is nonzero).
  Privileged processes bypass all kernel permission checks, while unpriv-
  ileged processes are subject to full permission checking based on the
  process's credentials (usually: effective UID, effective GID, and sup-
 plementary group list).

  Starting with kernel 2.2, Linux divides the privileges traditionally
  associated with superuser into distinct units, known as capabilities,
  which can be independently enabled and disabled. Capabilities are a
  per-thread attribute.

Capabilities list
  The following list shows the capabilities implemented on Linux, and the
  operations or behaviors that each capability permits:

  CAP_AUDIT_CONTROL (since Linux 2.6.11)
    Enable and disable kernel auditing; change auditing filter
    rules; retrieve auditing status and filtering rules.

  CAP_AUDIT_READ (since Linux 3.16)
    Allow reading the audit log via a multicast netlink socket.

  CAP_AUDIT_WRITE (since Linux 2.6.11)
    Write records to kernel auditing log.

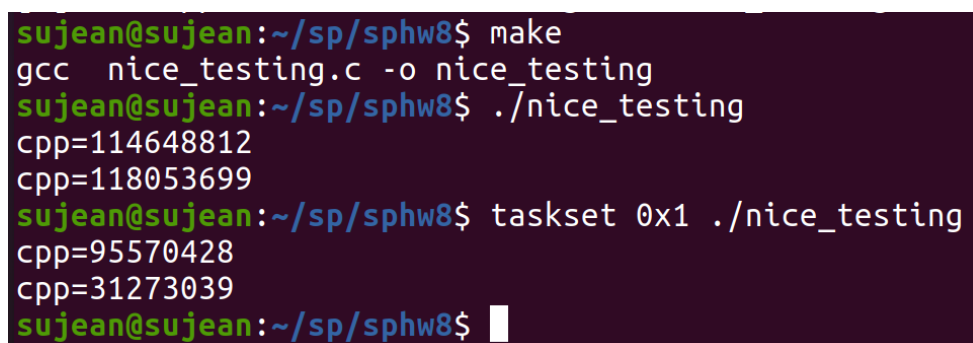
  CAP_BLOCK_SUSPEND (since Linux 3.5)
    Employ features that can block system suspend (epoll(7) EPOLL-
    WAKEUP, /proc/sys/wake_lock).

  CAP_CHOWN
    Make arbitrary changes to file UIDs and GIDs (see chown(2)).

Manual page capabilities(7) line 1 (press h for help or q to quit)
```

1. `CAP_AUDIT_CONTROL`：啟用和禁用 `kernal` 的審計功能，改變審計過濾規則，檢索審計狀態和過濾規則
2. `CAP_AUDIT_READ`：允許透過 `multicast netlink socket` 讀取審計日誌
3. `CAP_AUDIT_WRITE`：將記錄寫入 `kernal` 審計日誌

二、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』？



```
sujean@sujean: ~/sp/sphw8$ make
gcc nice_testing.c -o nice_testing
sujean@sujean: ~/sp/sphw8$ ./nice_testing
cpp=114648812
cpp=118053699
sujean@sujean: ~/sp/sphw8$ taskset 0x1 ./nice_testing
cpp=95570428
cpp=31273039
sujean@sujean: ~/sp/sphw8$
```

$$95570428/31273039 = 3.056$$

Nice 每一個等級差 1.25 倍， $1.25^5 = 3.05$

參考資料：

<https://iter01.com/554620.html>