系統程式設計 System Programming 2021

電機四 406415089 宋 O 天

Hw08 Chown_Super & Nice

<前置作業>

先執行 cp /usr/bin/chown ./chown_super

複製檔案 chown 變成 chown_super

再執行 sudo setcap CAP_CHOWN+ep ./chown_super

現在 chown_super 擁有更改任意檔案 owner 的權力

```
nash@SleepyCat: ~/Desktop/sp_hw
nash@SleepyCat:~/Desktop/sp_hw$ mv shown_super chown_super
nash@SleepyCat:~/Desktop/sp_hw$ ls
chown_super
nash@SleepyCat:~/Desktop/sp_hw$ sudo setcap CAP_CHOWN+ep ./chown_super
nash@SleepyCat:~/Desktop/sp_hw$
```

setcap : Capabilities 用於分割 root 用户的特權，將 root 的特權分割成不同的能力

這次用到的是 CAP_CHOWN： 修改文件主人的權限

執行./chown_super nash /usr/bin/ls 更改 ls 的使用者為 nash

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

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

<問題 1>

讓 nice_pro 擁有提高優先權的能力

一開始執行 ./nice_pro -n -10 ls 會出現 permission denied，這是因為只有 root 可以指定小於 0 的 niceness 值，一般使用者無法指定小於 0 的 niceness 值

我們需要 CAP_SYS_NICE 功能才能根據需要設置優先級

```
nash@SleepyCat: ~/Desktop/sp_hw
nash@SleepyCat:~/Desktop/sp_hw$ cp /usr/bin/nice ./nice_pro
nash@SleepyCat:~/Desktop/sp_hw$ ls
chown_super  nice_pro
nash@SleepyCat:~/Desktop/sp_hw$ ./nice_pro -n -10 ls
./nice_pro: cannot set niceness: Permission denied
chown_super  nice_pro
nash@SleepyCat:~/Desktop/sp_hw$
```

`sudo setcap CAP_SYS_NICE ./nice_pro` 會拿到提升優先權的權限

`sudo chmod +s ./nice+pro_2` 用之前學的 setuid 的方法會拿到整個 super user 的權限

```
nash@SleepyCat:~/Desktop/sp_hw$ sudo chown root ./nice_pro_2
nash@SleepyCat:~/Desktop/sp_hw$ sudo chmod+s ./nice_pro_2
sudo: chmod+s: command not found
nash@SleepyCat:~/Desktop/sp_hw$ sudo chmod +s ./nice_pro_2
nash@SleepyCat:~/Desktop/sp_hw$ ./nice_pro_2 -n -10 ls
chown_super  nice_pro  nice_pro_2
nash@SleepyCat:~/Desktop/sp_hw$
```

<問題 2>

想辦法量測 nice 提升優先權的比例

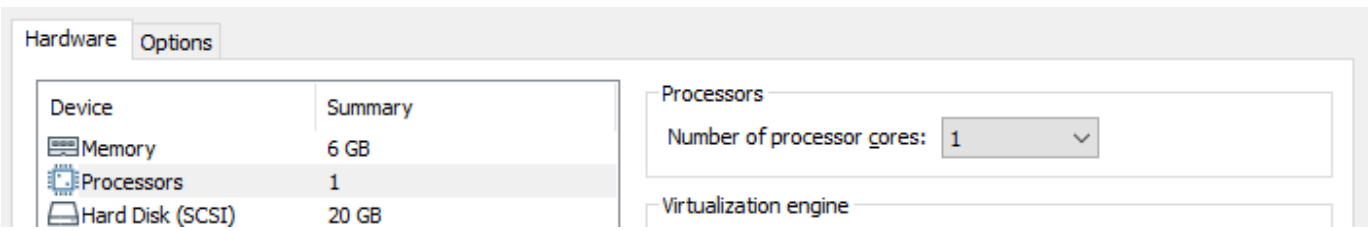
我的 code 是參考老師的 pseudo code (其實已經不能算 pseudo 的 code)寫的

因為還找不到讓 singal 傳帶有參數的函式的方法，只好把 pid 宣告成全域的

```
 6 long long int cpp = 0;
 7 int pid = 0;
 8
 9 void alarm_handler(int signo){
10     if(pid > 0)
11         printf("parent : ");
12     else
13         printf("child  : ");
14     printf("cpp = %lld\n", cpp);
15     exit(EXIT_SUCCESS);
16 }
                                                    6,1           17%
```

而且我的 vmware 的 processor 一開始就設定為 1，所以直接算就 OK

```
nash@SleepyCat:~/Desktop/sp_hw$ ./nice_testing 5
child  : cpp = 324998525
parent : cpp = 104975787
nash@SleepyCat:~/Desktop/sp_hw$ ./nice_testing 5
child  : cpp = 314829600
parent : cpp = 105527901
nash@SleepyCat:~/Desktop/sp_hw$
```



<回答問題>

<1>man capabilities

CAP_CHOWN
Make arbitrary changes to file UIDs and GIDs

隨意的更改檔案的 uid 和 gid

CAP_SYS_TIME
Set system clock (settimeofday(2), stime(2), adjtimex(2)); set real-time (hardware) clock.

設置系統時間(settimeofday(), stime()等)

CAP_SYSLOG (since Linux 2.6.37)
* Perform privileged syslog(2) operations. See syslog(2) for information on which operations require privilege.
* View kernel addresses exposed via */proc* and other interfaces when */proc/sys/kernel/kptr_restrict* has the value 1. (See the discussion of the *kptr_restrict* in proc(5).)

允許使用 syslog() 系統調用，在*/proc/sys/kernel/kptr_restrict* 設定為 1 的時候，可以藉/proc 和其他介面看到 kernel 的位址訊息

<2>從實驗結果算出提升比例

314829600 / 105527901 = 2.98　　log(2.98) = 0.4742

0.4742/5 = 0.09484　　X = 10^0.09484 = 1.244 倍

<參考資料>

https://www.cnblogs.com/sky-heaven/p/12096758.html

linux setcap 命令详解(包括各个 cap 的使用举例)【转】

https://blog.gtwang.org/linux/linux-nice-scheduling-priority/

Linux 的 nice 指令：指定程式執行的排程優先權（Scheduling Priority）

https://pxnet2768.pixnet.net/blog/post/71799543

linux 下 syslog 使用說明

https://man7.org/linux/man-pages/man7/capabilities.7.html

capabilities(7) — Linux manual page

<致謝>

羅 O 五老師