

國立中興大學 112-1 作業系統實驗 期中考試題

學號：

姓名：

測驗時間：60 分鐘

Part I. 筆試 (50%)

1. 請勾選正確的敘述 (12%，錯一個扣 2%)

- ☐ package 存在於 user space，當 package 要執行需要權限的操作(例如檔案讀寫) 之前，需要 system call，常見的 package 有 apt 和 gcc。
- ☐ kernel module 存在於 Kernel，它可以直接載入在執行中的 Kernel，常見的 kernel module 有 sudo。
- ☐ 任何跟 kernel module 有關的指令，最前面都需要加 sudo，只有 lsmod 和 dmesg 指令例外。
- ☐ socket 是一種允許 process 之間溝通的 interface，它的存在介於 transport layer 和 network layer 之間。
- ☐ 當 fork() 函式成功創建 child process 後，它會在 child process 中回傳 child process ID，在 parent process 回傳 0。
- ☐ 當呼叫 execlp() 函式後，原本的程式將主控權交給新的程式，等待新程式執行完畢後，再交還給原程式繼續執行。
- ☐ network byte order 是 **BIG** endian。
- ☐ Linux Kernel 是自由軟體，但是基於 Linux Kernel 開發出來的軟體並不見得也是。

178

2. 觀察以下程式，請把所有可能會輸出的順序寫出來 (5%)

1323

1233

2133

```
1 #include<stdio.h>
2 #include<sys/wait.h>
3 #include<unistd.h>
4
5 int main() {
6     pid_t pid;
7     pid = fork();
8     if (pid > 0) {
9         printf("2");
10        wait(NULL);
11    } else {
12        printf("1");
13    }
14    printf("3");
15
16    return 0;
17 }
```

3. purplelred (uid = 1000, 有 sudo 權限) 寫了一支 kernel module (12%)

```
purplelred@OSEnvironment:/home/share$ ls -al
total 16
drwxrwxrwx 2 root      root      4096  +- 26 16:44 
drwxr-xr-x 5 root      root      4096  +- 23 21:40 ..
-rw-rw-r-- 1 purplelred purplelred 152   +- 23 21:38 Makefile
-rw-rw-r-- 1 purplelred purplelred 348   +- 23 22:31 uid.c

1 // This is uid.c
2
3 #include<linux/cred.h>
4 #include<linux/module.h>
5
6 int init_module(void) {
7     struct cred *current_cred = get_current_cred();
8     kuid_t uid = current_cred->uid; // get current user's UID
9     printk(KERN_INFO "User ID %d inserts module uid. \n", uid.val);
10
11     return 0;
12 }
13
14 void cleanup_module(void) {
15     printk(KERN_INFO "Module uid has been removed. \n");
16 }
17
18 MODULE_LICENSE("GPL");
```

(1) 請寫出目前 terminal 所在的完整路徑 (也就是目前的工作路徑)。

(1%) /home/share

(2) 請寫出該路徑的存取權限。(三位數數字)

(1%) 777

(3) 如果要把當前路徑的存取權限改成 775, 要輸入什麼指令?

(1%) sudo chmod 775 .

(4) 請寫出 uid.c 的存取權限。(三位數數字)

(1%) 664

(5) purpleblue (uid = 1001) 想使用這個 terminal, 要輸入什麼指令?

(1%) su purpleblue

(6) 現在 purpleblue (有 sudo 權限)要編譯並安裝 uid.ko, 要輸入什麼指令?

(2%) 1. make 2. sudo insmod uid.ko

(7) Wait a minute... 他能成功嗎? (1%)

☐ Yes, 請跳過 (8) 並回答 (9) ☐ No, 請跳過 (9) Yes

(8) 為什麼 purpleblue 會安裝失敗?

(4%)

(9) 恭喜 purpleblue 成功安裝, 請問 dmesg 會印出什麼?

(4%) User ID 0 inserts module uid.

4. 請問什麼是 setuid？並舉出一個有使用 setuid 的檔案 (4%/2%)

setuid 是一個特殊的權限位，檔案有 setuid 屬性時，user 可以暫時使用 owner 的 ID 去執行程式而不是自己的，達到短暫的特權提升。

/usr/bin/passwd

5. 下圖是一個簡單的 sender/receiver 程式。其中圖(a) 有一個錯誤導致無法接收 sender 的訊息，請找出錯誤並解釋原因 (5%)

第 28 行是錯誤的，因為 $900 < \text{MAX_SIZE} = 1000$ ，需要修改 receiver 的 buffer size 讓他相等或是大於 sender 的 buffer size。

圖(a): receiver.c

```
1 #include<fcntl.h>
2 #include<mqueue.h>
3 #include<stdio.h>
4 #include<stdlib.h>
5 #include<string.h>
6 #include<sys/msg.h>
7 #include<sys/stat.h>
8 #include<sys/types.h>
9
10 #define MAX_SIZE 1000
11 #define MSG_STOP "/0"
12 #define NAME "/q2que"
13
14 int main(int argc, char **argv) {
15     char buffer[MAX_SIZE + 1];
16     int must_stop = 0;
17     struct mq_attr attr;
18     attr.mq_flags = 0;
19     attr.mq_maxmsg = 3;
20     attr.mq_msgsize = MAX_SIZE;
21     attr.mq_curmsgs = 0;
22     mqd_t mq1 = mq_open(NAME, O_RDONLY | O_CREAT, 0644, &attr);
23     if (mq1 == -1) {
24         perror("mq error:\n");
25         exit(1);
26     }
27     do {
28         ssize_t bytes_read = mq_receive(mq1, buffer, 900, NULL);
29         if (bytes_read < 0) {
30             perror("bytes_read error\n");
31             exit(1);
32         }
33         buffer[bytes_read] = '\0';
34         if (!strncmp(buffer, MSG_STOP, strlen(MSG_STOP))) {
35             must_stop = 1;
36         } else if (strcmp("exit\n", buffer) == 0) {
37             printf("received:%s", buffer);
38             must_stop = 1;
39         } else {
40             printf("received:%s", buffer);
41         }
42     } while (!must_stop);
43     mq_close(mq1);
44     mq_unlink(NAME);
45
46     return 0;
47 }
```

圖(b): sender.c

```
1 #include<fcntl.h>
2 #include<mqueue.h>
3 #include<stdio.h>
4 #include<stdlib.h>
5 #include<string.h>
6 #include<sys/msg.h>
7 #include<sys/stat.h>
8 #include<sys/types.h>
9
10 #define MAX_SIZE 1000
11 #define MSG_STOP "/0"
12 #define NAME "/q2que"
13
14 int main(int argc, char **argv) {
15     char buffer[MAX_SIZE];
16     mqd_t mq1 = mq_open(NAME, O_WRONLY | O_CREAT, 0644, NULL);
17     if (mq1 == -1) {
18         perror("mq1 error:\n");
19         exit(1);
20     }
21     printf("send to receiver:\n");
22     do {
23         for(int i = 0; i < sizeof(buffer); i++) {
24             buffer[i] = '\0';
25         }
26         printf(">");
27         fgets(buffer, MAX_SIZE, stdin);
28         int send = mq_send(mq1, buffer, strlen(buffer) + 1, 0);
29         if(send < 0) {
30             perror("message:\n");
31             exit(1);
32         }
33     } while(1);
34
35     return 0;
36 }
```

6. 在 shared memory 應用當中，ftruncate() 是否為必要的？另外它在創建/使用 shared memory 的過程中，ftruncate() 的功能為何？ (3%)
- 是，ftruncate() 是用來 resize 一定空間來應用 shared memory。

7. 請寫出下列程式碼的輸出

- (1) echo "`echo hi`" (2%) hi
- (2) echo "echo hi" (2%) `echo hi`

8. 請修改以下程式，使其可以輸出如右邊的結果 (3%)

程式：

```
for (( &i = 1; &i <= 9; &i += 2 )) 將&刪掉
do
    echo 'i = $i' 將單引號改成雙引號
done
```

結果：

i = 1
i = 3
i = 5
i = 7
i = 9