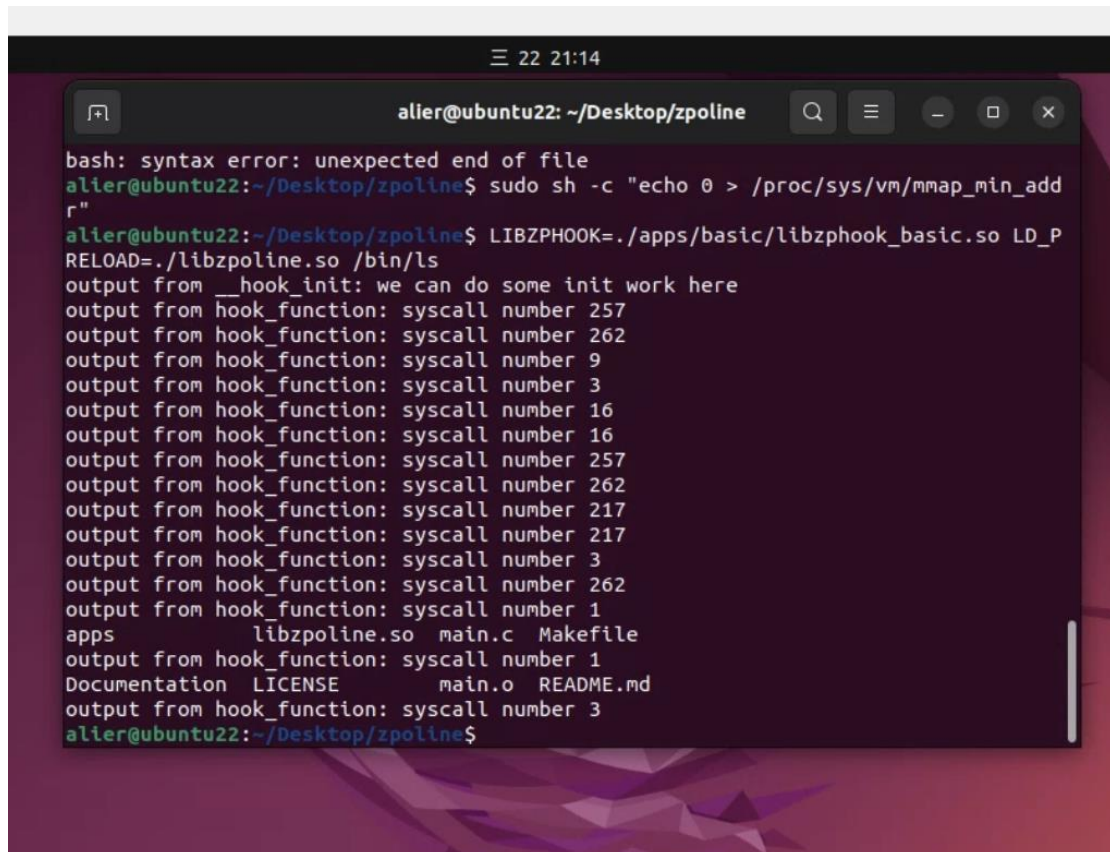


# Project 1 User-Level System Call Hook Report

312706026 資管所 曾雅鈺

## Task I

a.

A terminal window titled 'alier@ubuntu22: ~/Desktop/zpoline' with a search bar and window controls. The terminal shows a sequence of commands and outputs. First, a 'bash: syntax error: unexpected end of file' message is shown. Then, the user runs 'sudo sh -c "echo 0 > /proc/sys/vm/mmap\_min\_addr"', which succeeds. Next, the user runs 'LIBZPHOOK=./apps/basic/libzphook\_basic.so LD\_PRELOAD=./libzpoline.so /bin/ls'. The output shows the standard 'ls' output for the directory contents, with each line prefixed by 'output from hook\_function: syscall number'. The syscall numbers are: 257, 262, 9, 3, 16, 16, 257, 262, 217, 217, 3, 262, 1, 1, 1, 3. The terminal background has a purple and blue geometric pattern.

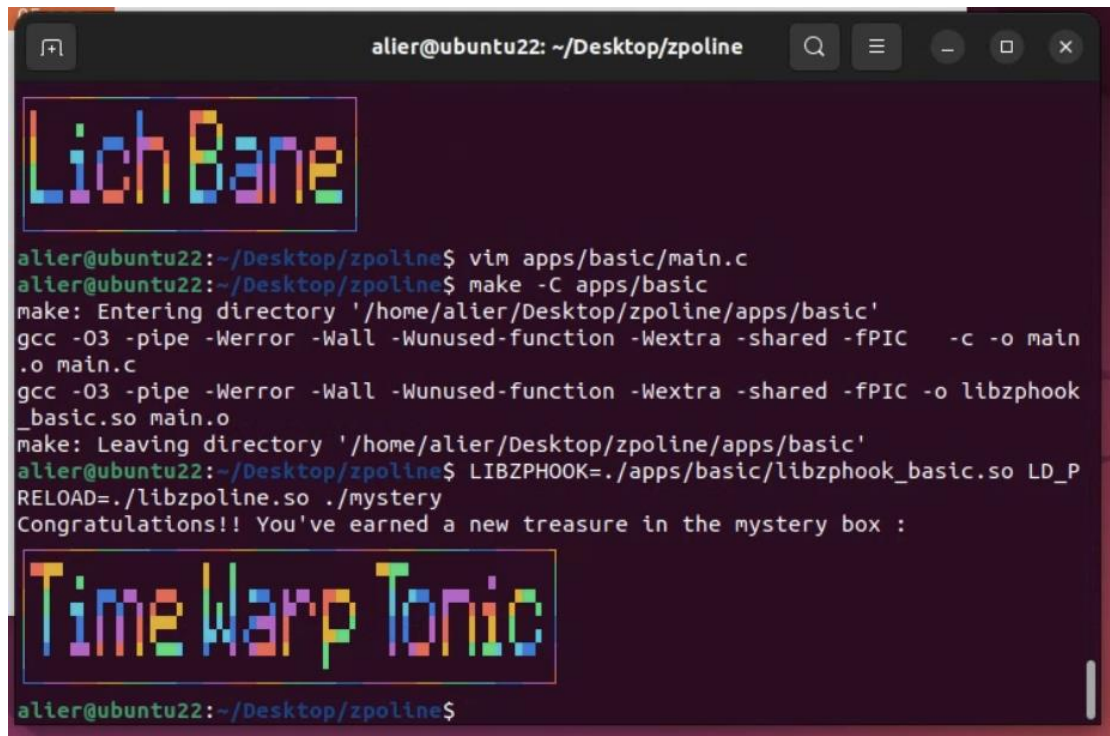
```
bash: syntax error: unexpected end of file
alier@ubuntu22:~/Desktop/zpoline$ sudo sh -c "echo 0 > /proc/sys/vm/mmap_min_addr"
alier@ubuntu22:~/Desktop/zpoline$ LIBZPHOOK=./apps/basic/libzphook_basic.so LD_PRELOAD=./libzpoline.so /bin/ls
output from __hook_init: we can do some init work here
output from hook_function: syscall number 257
output from hook_function: syscall number 262
output from hook_function: syscall number 9
output from hook_function: syscall number 3
output from hook_function: syscall number 16
output from hook_function: syscall number 16
output from hook_function: syscall number 257
output from hook_function: syscall number 262
output from hook_function: syscall number 217
output from hook_function: syscall number 217
output from hook_function: syscall number 3
output from hook_function: syscall number 262
output from hook_function: syscall number 1
apps      libzpoline.so  main.c  Makefile
output from hook_function: syscall number 1
Documentation  LICENSE      main.o  README.md
output from hook_function: syscall number 3
alier@ubuntu22:~/Desktop/zpoline$
```

b.

‘getdents64’ system call is used by /bin/ls to retrieve file and directory names.

## Task II

a.



```
alier@ubuntu22: ~/Desktop/zpoline
Lich Bane
alier@ubuntu22:~/Desktop/zpoline$ vim apps/basic/main.c
alier@ubuntu22:~/Desktop/zpoline$ make -C apps/basic
make: Entering directory '/home/alier/Desktop/zpoline/apps/basic'
gcc -O3 -pipe -Werror -Wall -Wunused-function -Wextra -shared -fPIC -c -o main.o main.c
gcc -O3 -pipe -Werror -Wall -Wunused-function -Wextra -shared -fPIC -o libzphook_basic.so main.o
make: Leaving directory '/home/alier/Desktop/zpoline/apps/basic'
alier@ubuntu22:~/Desktop/zpoline$ LIBZPHOOK=./apps/basic/libzphook_basic.so LD_PRELOAD=./libzpoline.so ./mystery
Congratulations!! You've earned a new treasure in the mystery box :
Time Warp Tonic
alier@ubuntu22:~/Desktop/zpoline$
```

b. 先印出所有 system call 的參數並觀察找到 system call 59，當 a1 等於 59 時，印出它的 a3 內容，觀察它的內容後，在正確位置添加--gay，並在--gay 後面添加 NULL。

我覺得這樣可能會有風險，因為修改的過程很複雜且容易出錯，會增加系統出錯的風險，且可能會引入安全漏洞。因此還是要儘量避免修改 vDSO memory mapping。

### Difficulties I encountered

1. 一開始使用 Mac 按照步驟裝系統，但執行時會一直出現無法找到 x86\_64 指令的問題，因為不知道該如何解決，最後換成使用 Windows 系統。
2. 在安裝 ubuntu 22.04 時，一開始有出現 Kernel Panic - not syncing: VFS: Unable to mount root fs on unknown-block(0, 0)的問題，查詢後發現是 boot 空間已滿載，對內部進行清理後，問題解決。
3. 接續問題 2，一開始出現問題時，直接換成 ubuntu 20.04，但到 Task II 時，出現 GLIBC\_2.34 not found 的問題，發現是版本問題，因此先對 GLIBC 升級，但完成升級後會出現.so 檔案無法找到的問題，直接用指令升級 ubuntu22.04 也無法解決，最後去解決問題 2 直接安裝 ubuntu22.04。
4. 一開始不知道 main.c 如何修改，之後有陸續詢問助教，通過助教的提示有慢慢理解，最後修改成功！謝謝助教！