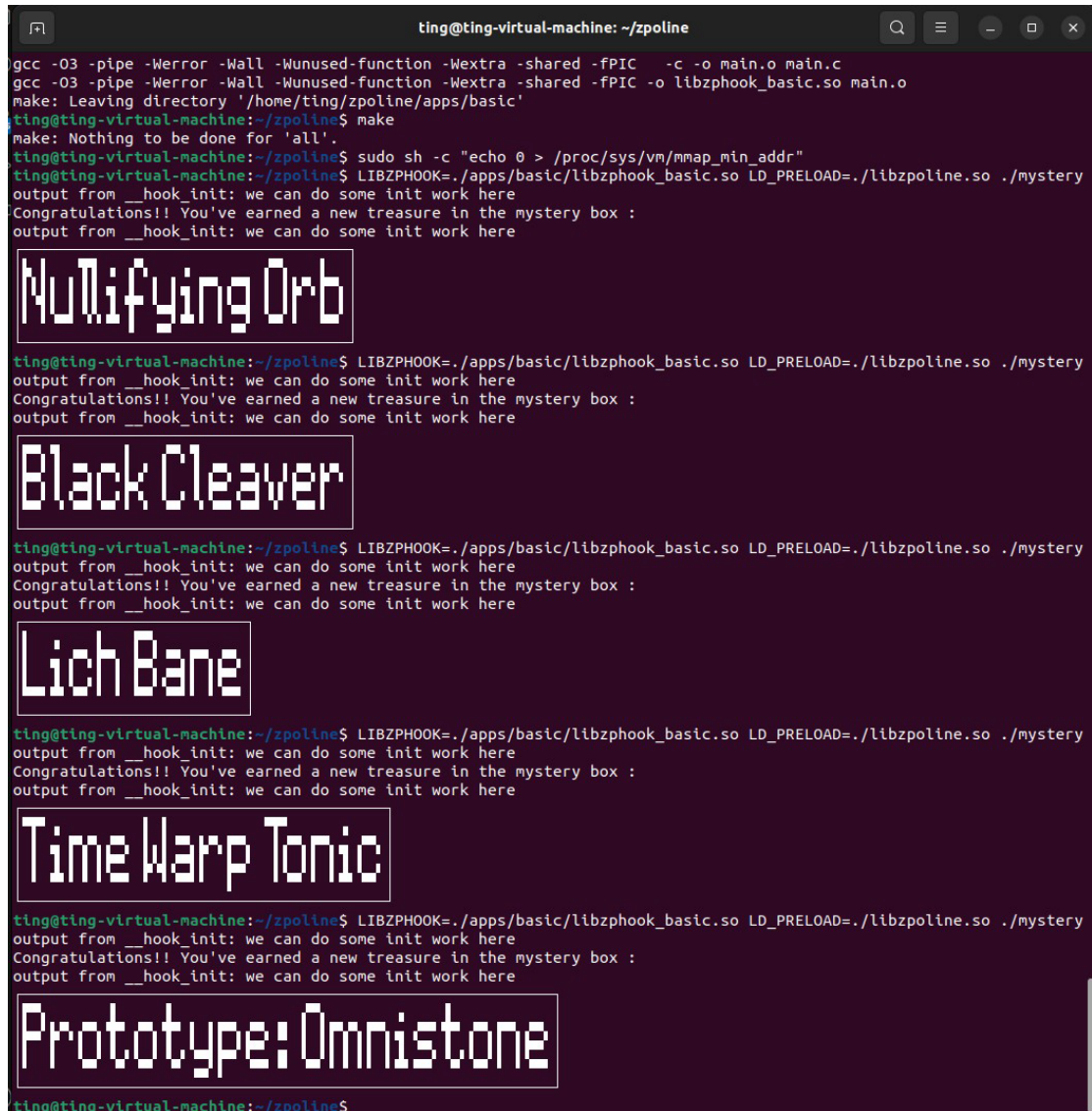


# Project 1 User-Level System Call Hook Report

312706038 資管所 吳方庭

## #Task I

- a. A screenshot of your output.



```
ting@ting-virtual-machine: ~/zpoline
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/ting/zpoline/apps/basic'
ting@ting-virtual-machine:~/zpoline$ make
make: Nothing to be done for 'all'.
ting@ting-virtual-machine:~/zpoline$ sudo sh -c "echo 0 > /proc/sys/vm/mmap_min_addr"
ting@ting-virtual-machine:~/zpoline$ LIBZPHOOK=./apps/basic/libzphook_basic.so LD_PRELOAD=./libzpoline.so ./mystery
output from __hook_init: we can do some init work here
Congratulations!! You've earned a new treasure in the mystery box :
output from __hook_init: we can do some init work here
Nullifying Orb
ting@ting-virtual-machine:~/zpoline$ LIBZPHOOK=./apps/basic/libzphook_basic.so LD_PRELOAD=./libzpoline.so ./mystery
output from __hook_init: we can do some init work here
Congratulations!! You've earned a new treasure in the mystery box :
output from __hook_init: we can do some init work here
Black Cleaver
ting@ting-virtual-machine:~/zpoline$ LIBZPHOOK=./apps/basic/libzphook_basic.so LD_PRELOAD=./libzpoline.so ./mystery
output from __hook_init: we can do some init work here
Congratulations!! You've earned a new treasure in the mystery box :
output from __hook_init: we can do some init work here
Lich Bane
ting@ting-virtual-machine:~/zpoline$ LIBZPHOOK=./apps/basic/libzphook_basic.so LD_PRELOAD=./libzpoline.so ./mystery
output from __hook_init: we can do some init work here
Congratulations!! You've earned a new treasure in the mystery box :
output from __hook_init: we can do some init work here
Time Warp Tonic
ting@ting-virtual-machine:~/zpoline$ LIBZPHOOK=./apps/basic/libzphook_basic.so LD_PRELOAD=./libzpoline.so ./mystery
output from __hook_init: we can do some init work here
Congratulations!! You've earned a new treasure in the mystery box :
output from __hook_init: we can do some init work here
Prototype: Omnistone
ting@ting-virtual-machine:~/zpoline$
```

- b. Describe which system call is used by `/bin/ls` to retrieve file and directory names.

ANS: The `sys_getdents` system call in Linux is used to retrieve directory entries from a file descriptor that refers to a directory.

## #Task II

- a. A screenshot of your output.

```

Congratulations!! You've earned a new treasure in the mystery box :
output from __hook_init: we can do some init work here

Mercurial Scimitar

ting@ting-virtual-machine:~/zpolines$ LIBZPHOOK=./apps/basic/libzphook_basic.so LD_PRELOAD=./libzpoline.so ./mystery
output from __hook_init: we can do some init work here
Congratulations!! You've earned a new treasure in the mystery box :
output from __hook_init: we can do some init work here

Nimbus Cloak

ting@ting-virtual-machine:~/zpolines$ LIBZPHOOK=./apps/basic/libzphook_basic.so LD_PRELOAD=./libzpoline.so ./mystery
output from __hook_init: we can do some init work here
Congratulations!! You've earned a new treasure in the mystery box :
output from __hook_init: we can do some init work here

Duskblade of Draktharr

ting@ting-virtual-machine:~/zpolines$ LIBZPHOOK=./apps/basic/libzphook_basic.so LD_PRELOAD=./libzpoline.so ./mystery
output from __hook_init: we can do some init work here
Congratulations!! You've earned a new treasure in the mystery box :
output from __hook_init: we can do some init work here

Arcane Comet

ting@ting-virtual-machine:~/zpolines$ LIBZPHOOK=./apps/basic/libzphook_basic.so LD_PRELOAD=./libzpoline.so ./mystery
output from __hook_init: we can do some init work here
Congratulations!! You've earned a new treasure in the mystery box :
output from __hook_init: we can do some init work here

Rod of Ages
```

- b. Describe how you design hook\_function to modify the appearance of your treasures.

- 要先觀察哪個 system call 比較適合做 hook，找到 syscall:59。
- system call table 有列出所有 system call 的參數，%rdi~%r9 對應 source code 裡的 a2~a7。
- 在 execve 的 a3，可以看出所有的參數，如下圖。

```

ting@ting-virtual-machine:~/zpolines$ LIBZPHOOK=./apps/basic/libzphook_basic.so LD_PRELOAD=./libzpoline.so ./mystery
output from __hook_init: we can do some init work here
Congratulations!! You've earned a new treasure in the mystery box :
140727834668432
argv[0] = toilet
argv[1] = -f
argv[2] = smbblock
argv[3] = -F
argv[4] = border
argv[5] = Nullifying Orb
140727834668432
argv[0] = toilet
argv[1] = -f
argv[2] = smbblock
argv[3] = -F
argv[4] = border
argv[5] = Nullifying Orb
```

- 最後補上 argv[6]和 argv[7]，就可以完成呼叫 toilet 套件了。

```

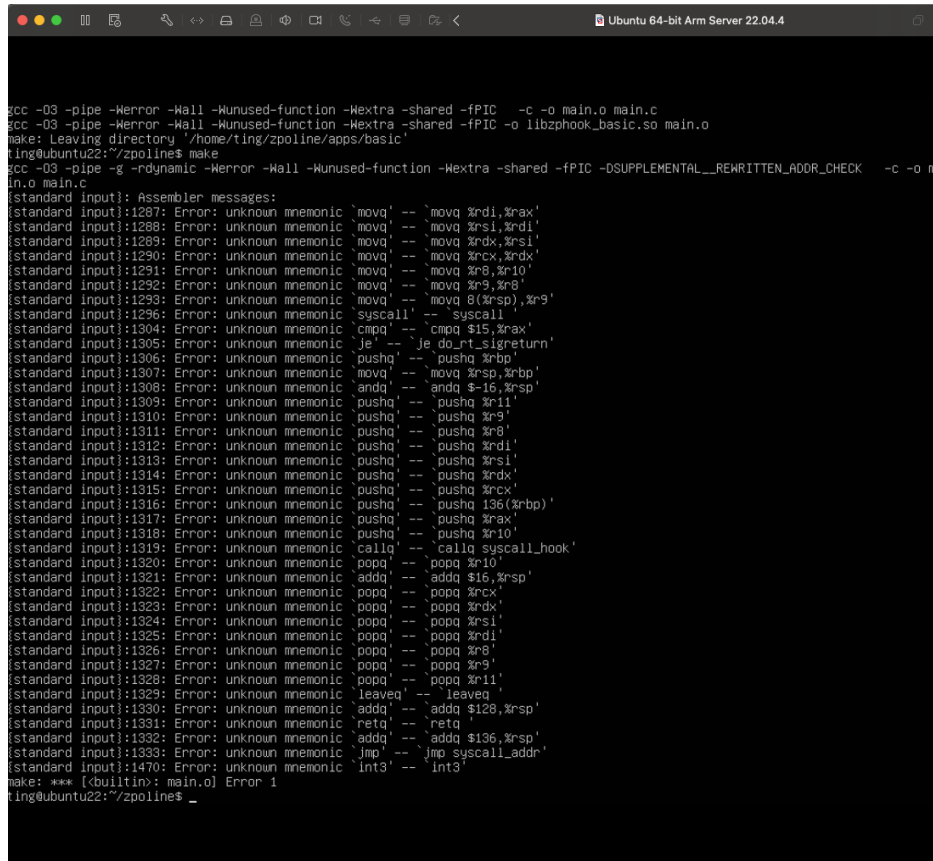
const char **args = (const char **)a3;
args[6] = "--gay";
args[7] = NULL;
```

**#Q1:** In the paper, they mentioned that zpoline cannot hook vDSO-based system calls. Do you think performing a binary patch on the vDSO memory mapping inside the hooked process is a feasible solution? Provide your reasoning.

ANS: 要在 vDSO 上映射執行 binary patch 是可行的，但由於 vDSO 記憶體映射通常標記為唯讀，可能還會設有更多的安全性保護措施，所以要去修改它必須先避開這些保護，這種方法會帶來很多安全的風險，也可能造成系統不穩定，所以我認為不適合這麼做。

#Q2: Describe difficulties you encountered in the implementations and how you have addressed them.

- 此次作業使用的套件需要在 Ubuntu 22.04 x86\_64 才能運行，但因為 Mac m2 是沒有 support x86\_64，除非另外安裝。但後來我嘗試過太多次還是無法運行，最後換成 Windows 系統。

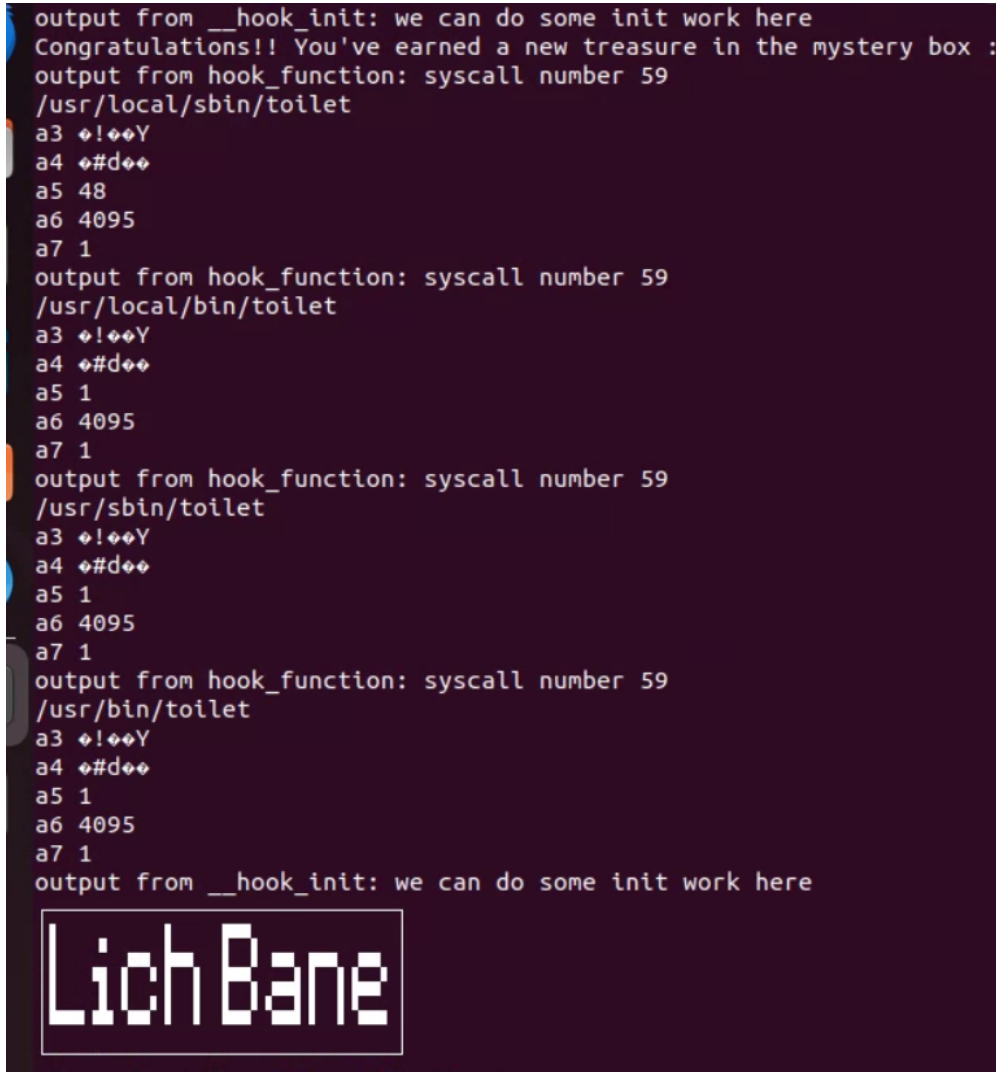


```
gcc -O3 -pipe -Werror -Wall -Wunused-function -Wextra -shared -fPIC -c -o main.o main.c
gcc -O3 -pipe -Werror -Wall -Wunused-function -Wextra -shared -fPIC -o libzphook_basic.so main.o
make: Leaving directory '/home/ting/zpoline/apps/basic'
tingubuntu22:~/zpoline$ make
gcc -O3 -pipe -g -rdynamic -Werror -Wall -Wunused-function -Wextra -shared -fPIC -DSUPPLEMENTAL__REWRITTEN_ADOR_CHECK -c -o main.o main.c
[standard input]: Assembler messages:
[standard input]:1287: Error: unknown mnemonic `movq' -- `movq %rdi,%rax'
[standard input]:1288: Error: unknown mnemonic `movq' -- `movq %rsi,%rdi'
[standard input]:1289: Error: unknown mnemonic `movq' -- `movq %rdx,%rsi'
[standard input]:1290: Error: unknown mnemonic `movq' -- `movq %rcx,%rdx'
[standard input]:1291: Error: unknown mnemonic `movq' -- `movq %r8,%r10'
[standard input]:1292: Error: unknown mnemonic `movq' -- `movq %r9,%r8'
[standard input]:1293: Error: unknown mnemonic `movq' -- `movq 8(%rsp),%r9'
[standard input]:1296: Error: unknown mnemonic `syscall' -- `syscall'
[standard input]:1304: Error: unknown mnemonic `cmovq' -- `cmovq %15,%rax'
[standard input]:1305: Error: unknown mnemonic `je' -- `je do_rt_sigreturn'
[standard input]:1306: Error: unknown mnemonic `pushq' -- `pushq %rbp'
[standard input]:1307: Error: unknown mnemonic `movq' -- `movq %rsp,%rbp'
[standard input]:1308: Error: unknown mnemonic `andq' -- `andq $-16,%rsp'
[standard input]:1309: Error: unknown mnemonic `pushq' -- `pushq %r11'
[standard input]:1310: Error: unknown mnemonic `pushq' -- `pushq %r9'
[standard input]:1311: Error: unknown mnemonic `pushq' -- `pushq %r8'
[standard input]:1312: Error: unknown mnemonic `pushq' -- `pushq %rdi'
[standard input]:1313: Error: unknown mnemonic `pushq' -- `pushq %rsi'
[standard input]:1314: Error: unknown mnemonic `pushq' -- `pushq %rdx'
[standard input]:1315: Error: unknown mnemonic `pushq' -- `pushq %rcx'
[standard input]:1316: Error: unknown mnemonic `pushq' -- `pushq 136(%rbp)'
[standard input]:1317: Error: unknown mnemonic `pushq' -- `pushq %rax'
[standard input]:1318: Error: unknown mnemonic `pushq' -- `pushq %r10'
[standard input]:1319: Error: unknown mnemonic `callq' -- `callq syscall_hook'
[standard input]:1320: Error: unknown mnemonic `popq' -- `popq %r10'
[standard input]:1321: Error: unknown mnemonic `addq' -- `addq %16,%rsp'
[standard input]:1322: Error: unknown mnemonic `popq' -- `popq %rcx'
[standard input]:1323: Error: unknown mnemonic `popq' -- `popq %rdx'
[standard input]:1324: Error: unknown mnemonic `popq' -- `popq %rsi'
[standard input]:1325: Error: unknown mnemonic `popq' -- `popq %rdi'
[standard input]:1326: Error: unknown mnemonic `popq' -- `popq %r8'
[standard input]:1327: Error: unknown mnemonic `popq' -- `popq %r9'
[standard input]:1328: Error: unknown mnemonic `popq' -- `popq %r11'
[standard input]:1329: Error: unknown mnemonic `leaveq' -- `leaveq'
[standard input]:1330: Error: unknown mnemonic `addq' -- `addq %128,%rsp'
[standard input]:1331: Error: unknown mnemonic `retq' -- `retq'
[standard input]:1332: Error: unknown mnemonic `addq' -- `addq %136,%rsp'
[standard input]:1333: Error: unknown mnemonic `jmp' -- `jmp syscall_addr'
[standard input]:1470: Error: unknown mnemonic `int3' -- `int3'
make: *** [builtin: main.o] Error 1
tingubuntu22:~/zpoline$
```

- 同時，我也使用 Lab 的 Linux 系統跑實驗，而 Lab 的 Linux 系統是 Ubuntu 20.04 版本，安裝 Zpoline 套件運行的很順利，但是在跑 mystery 執行檔時，遇到 GLIBC\_2.34 not found 的問題，有嘗試解決但是因為不是沒有 root 權限也不能處理。
- 後來，換在 Windows 系統上用 WSL 安裝 Ubuntu 22.04，但又遇到 sh: 1: cannot create /proc/sys/vm/mmap\_min\_addr: Operation not permitted 的問題。
- 最後在 Windows 上裝 VM，剛下載完 VM 打開 app 時直接 shutdown，應用程式完全無法打開。後來，是更改在 Intel 主機板通過更改 BIOS 並開啟虛擬化功能才能正常運行。
- 接下來遇到的問題，是不確定要如何將 hook 到的內容輸出成彩色。過程有詢問助教及同學，也得到一些提示 → “彩色字型可以透過設定 toilet 的參數來完成，另外要觀察一下哪個 system call 比較適合做 hook。”

- 讀取 syscall(目前讓 a1==59 後)，有嘗試使用 system("echo 'output from hook\_function: syscall number 59' | toilet --gay");去設定 toilet 參數，但執行後會無法暫停。發現這問題是因為在 hook\_function 內呼叫 system()會產生無權迴圈。
- 參數透過轉換後有得出這個結果(如下圖)，也找到 syscall 59 的 a2 是 toilet 的指標，想要設定 toilet 參數在 a2 裡面，但因為印出來的每個路徑都不同，所以不知道要如何設定？

```
output from __hook_init: we can do some init work here
Congratulations!! You've earned a new treasure in the mystery box :
output from hook_function: syscall number 59
/usr/local/sbin/toilet
a3 ❖!❖❖Y
a4 ❖#d❖❖
a5 48
a6 4095
a7 1
output from hook_function: syscall number 59
/usr/local/bin/toilet
a3 ❖!❖❖Y
a4 ❖#d❖❖
a5 1
a6 4095
a7 1
output from hook_function: syscall number 59
/usr/sbin/toilet
a3 ❖!❖❖Y
a4 ❖#d❖❖
a5 1
a6 4095
a7 1
output from hook_function: syscall number 59
/usr/bin/toilet
a3 ❖!❖❖Y
a4 ❖#d❖❖
a5 1
a6 4095
a7 1
output from __hook_init: we can do some init work here
```



- 解決辦法：execve 的 syscall 是因為 mystery 的原始碼用的是 execlp function 去執行 toilet，系統會去環境變數 PATH 的路徑底下，一個個找 toilet 執行檔來執行。
- 最後，實在太感謝助教的幫助，非常有耐心的引導我去理解整個 project 的過程，謝謝你！！