

## Task 1:

```
karrs@nspj24:~/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 Documentation libzpoline.so LICENSE main.c main.o Makefile README.md
output from hook_function: syscall number 3
```

257 是 `sys_openat`，是開啟檔案。262 是 `sys_newfstatat`，可以取得目標檔案的各種資訊。9 是 `sys_mmap`，會打開一個 virtual memory 的 page。3 是 `close`，會將指定的 fd 關掉。16 是 `sys_ioctl`，會針對指定的 command 行動。217 是 `sys_getdents64`，會從指定資料夾中取出 `linux_dirent` 的資料。1 是 `write`，會對指定的 fd 做寫入。

## Task 2:

```
karrs@nspj24:~/zpoline$ LIBZPHOOK=./apps/basic/libzphook_basic.so LD_PRELOAD=./libzpoline.so ./mystery
Congratulations!! You've earned a new treasure in the mystery box :
ManaflowBand

karrs@nspj24:~/zpoline$ LIBZPHOOK=./apps/basic/libzphook_basic.so LD_PRELOAD=./libzpoline.so ./mystery
Congratulations!! You've earned a new treasure in the mystery box :
Arcane Comet

karrs@nspj24:~/zpoline$ LIBZPHOOK=./apps/basic/libzphook_basic.so LD_PRELOAD=./libzpoline.so ./mystery
Congratulations!! You've earned a new treasure in the mystery box :
Hextech Flashtraction

karrs@nspj24:~/zpoline$
```

再查看 `toilet` 的時候，看到了 `gay` 這個 filter 的效果和題目敘述的一樣，因此就去查看 `mystery` 裡面有沒有去下 `toilet` 的指令，找到 59 號是 `sys_execve`，並且因為他的參數是放在 `a3` 的地方，找到他原先下的指令為 `toilet -f smbblock -F border {文字}`，因此我將 `border` 改成 `border:gay`，並且繼續執行 system call。

我認為應該是可行的，因為要成功的話，最主要就是要將其導入到我們想要的位置，因此如果可以在跳轉的時候，重新導向至 `system call`，就能進入 `trampoline code`，並且成功的 `hook function`，也就是說設計一段程式，內容是跳轉是我們想要的地方，應該就能成功。

我覺得這次作業的難點在於不太知道要如何下手，像是我一開始是打算再呼叫 `sys_write` 下手，後來在看 `mystery` 做出了哪些 `system call` 時，發現可以在 `sys_execve` 時下手，並且更加簡潔，且一旦知道如何取得想要的資料後，就可以加以修改，並且完成作業。