CS: hw4 - hacknote2

學號：b04902053 姓名：鄭淵仁

flag: `FLAG{DEATHNOTE!!!!}`

script

- 可以取得 shell 的 python3 檔案： `hacknote2.py`

  (requirements: pwntools)

write-up

程式的漏洞

`hacknote2` 在 free 掉內容之後沒有把 pointer 的值設回 `NULL` ，所以可以 use after free 。

leak 出 `libc` 的位置

首先製造 2 個 `note` 再 free 掉。之後再新增一個大小和 `printnote` 一樣大 (8 byte) 的 `content` ，這個 `content` 就會分配到之前 free 掉的第 0 個 `note` 的 `printnote` 。這時候就可以用第 2 個 `note` 的 `content` 來寫入 address ，然後用第 0 個 `note` 的 `printnote` 來 call 那個 address 。

所以要寫入的 `content` 就選擇是 `print_note_content()` ，後面再寫入 `puts` 在 got 上的位置。如此一來就會 puts 出 `puts` 的 address ，這樣就可以推算出 `libc` 的位置了。

call `execve(";/bin/sh", 0, 0)`

在這裡我使用套件 `one_gadget` 來在 `libc` 裡面找到可以直接執行 `execve(";/bin/sh", 0, 0)` 的 gadget 。再來就是把找到的 address 放到第 2 個 `note` 的 `content` 裡面，就可以用第 0 個 `note` 的 `printnote` 來執行 `execve(";/bin/sh", 0, 0)` 了。