hacknote - pwnable.tw

b04902053 鄭淵仁

flag

```
FLAG{Us3_aft3r_fl3333_in_h4ck_not3}
```

solution

這一題和 `csie.ctf.tw` 裡面的作業 4 幾乎一樣，就只有差在這一題的 architecture 是 `i386` 。

所以這一題的 address 不會有 null byte，所以這一題最後不需要使用 `one_gadget` ，可以傳 `system` 的 address 之後再加上 `";sh"` 就可以了。

下面是我在作業 4 時使用的方法，我把使用 `one_gadget` 的敘述改成使用 `system` 之後就如下：

程式的漏洞

`hacknote` 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 `system("[system];sh")`

在這裡我把 `system` 的 address 和 `";sh"` 放到第 2 個 `note` 的 `content` 裡面，這樣就可以用第 0 個 `note` 的 `printnote` 來讓 `bash` 執行 `system` 的 address 以及 `sh` 了。

script

- `hacknote.py` : 可以拿到 shell 的 python3 script。