hw2 write-up - Computer Security

學號：b04902053

姓名：鄭淵仁

write-up

`gothijack` 這支程式一共會讀三次 input，而且沒有開啟 `NX` 保護機制。

第一次讀 input 的時候，程式會使用 `read()` 固定讀 48 個 char 到一個 global variable，但是在 `check()` 的時候，卻只檢查表格裡面 index 小於 `strlen()` 的元素是不是字母或數字。這代表 `check()` 在檢查到 `'\0'` 之後就會停下來了，而不管 `'\0'` 後面讀入的其他 char。

所以我就在第一次要 input 的時候先給他 `'\0'`，接下來再給開 `/bin/sh` 的 shell code。這樣一來程式就不會檢查到 `'\0'` 後面的不是字母或數字的 shell code 了。

接下來第二次 input 的時候就給他 GOT 裡面 `puts()` 的位置，第三次 input 的時候就可以給之前寫入的 shell code 的位置。

這樣就可以把 GOT 裡面 `puts()` 的位置改寫成之前寫入的 shell code 的位置，也就是說，在最後執行 `puts("done!")` 的時候，就會變成執行 `execve("/bin/sh")`，就可以取得 shell 了。

script

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