

# hw0 - Computer Security 2017 Fall

---

學號：b04902053

姓名：鄭淵仁

## pwn1

---

先用 `objdump`，發現有用到 `gets`，可以 overflow 它，另外也找到一個 function - `callme`。看起來就是要用 `gets` 去 overflow `stack`，以覆蓋 `return` address，讓程式在 `return` 的時候改成執行 `callme`。

接著檢查 `CANARY`，發現是 disabled 的，所以就直接用 `pwntools` 裡面的 `cyclic` 算出 `gets` 寫入的位置和 `return` address 之間的 offset，然後用 `gets` 把 `callme` 的 address 寫到那裡就可以了。

可以連上工作站取得 `sh` 的檔案：`pwn1.py`

## BubbleSort

---

先用 `objdump`，發現有一個 function - `DarkSoul`，看起來就是要執行他。

接著實際跑這個程式，發現程式雖然會檢查要 `sort` 的元素的上限，卻不會檢查下限，所以就給他負值看看，結果再搭配 `gdb` 會發現程式後來會把負值轉成 `unsigned`，就變成可以 `sort` 到 `stack` 後面的值。

接著檢查 `CANARY`，發現是 disabled 的，所以就一次輸入 127 個 `DarkSoul` 的 address，並且 `sort` -1 個元素，來把 address 蓋到 `stack` 裡面的 `return` address 上面。

可以連上工作站取得 `sh` 的檔案：`BubbleSort.py`

## rev1

---

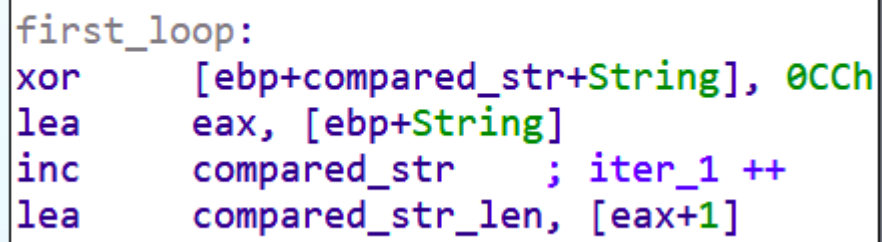
先用 `objdump`，發現有一個 function - `print_flag`，而且 function 的內容很明顯是把一個一個 `char` 移進一個 `array`，仔細檢查會發現 function 有照順序把 `char` 放進去，所以就把那些 `char` 的值從 `hex` 轉回 `utf-8`，就是 flag 了。

## rev2

---

用 `ida_pro` 打開程式，先改程式流程讓他直接 print 答案，結果他只給一個 "Congrat" 的訊息，之後就沒有了，所以重點不是要 print 出答案，而是要找出密碼。

所以仔細觀察程式驗證密碼的過程，發現他先把輸入的值跟 `0xCC` `xor`，之後再跟程式內的 data 比較。所以就把程式內的 data 跟 `0xCC` `xor` 就可以得到密碼，最後發現密碼其實就是 flag。



```
first_loop:
xor      [ebp+compared_str+String], 0CCh
lea      eax, [ebp+String]
inc      compared_str      ; iter_1 ++
lea      compared_str_len, [eax+1]
```

(程式裡面，跟 0xCC xor 的程式碼)