計算機安全 HW 0x0a Writeup

- Real name: 張瀚文
- Nickname on course website: Hwww
- Student ID: b07505027.

Survey

解法

這題明顯跟ROPlab類似，但這題的限制更多，只能有兩次輸入輸出，然後因為seccomp的關係，只能用限定的syscall，也就不能直接拿到shell，要用open, read, write等。這題用 `checksec` 看，知道保護機制全開了，有canary, pie等，因此在ROP之前也要先leak出canary跟base。

leak canary, code base. stack pivot, rbp to bss

在第一次輸入的時候，剛好可以leak出canary跟某個PIE過的位址，可以推算出code base。

有了code base後，可以先計算出一些會用到的gadget，如：main_body, bss, leave等，稍後會用到

接下來因為能輸入的次數只剩下一次，但我們能寫的ROP有限，還沒有libc，ROP長度也因為程式只能讀0x30大小而被受限（扣掉canary等只能寫一個gadget），因此要利用stack pivot來創造更多空間。而我們可以將fakerbp改成一個我們可以控制的空間，像是bss(0x4000 ~ 0x5000)，通常是可寫的，然後將ROPchain放入main中輸入的部分，如此一來又可以再重新輸入，並且stack已經被搬到bss上了。

send nothing to leave address in bss

在這一步隨便送一些東西，目的只是為了讓程式能在bss中留下一些位址，像是我們要的libc，然後再stack piovt一次，回來重新輸入leak libc。

ready to leak libc in bss. stack pivot to long ROP chain

這時候利用跟leack canary一樣的方法來leak libc，並計算一些之後會用到的gadget，如gets, pop_rdi, syscall等

接下來要製造一個可以寫入很長的ROPchain的空間，來讓我們寫open, read, write來拿到flag。而同樣也可以用stack pivot來製造。但因為輸入的長度有限，所以頂多只能長到放三個指令，所以必須利用這三個gadget再製造可以輸入更長的ROPchain的地方。

製造三個gadget的方法跟pwn1上課時講的方法幾乎類似，準備好的ROPchain利用輸入放到bss中，fackrbp則放長ROPchain - fackrbp2 的位址，最後leave來stack pivot，就可以執行長ROPchain。而這裡放了gets在ROPchain中，並且gets input的buffer直接接在gets()結束後，所以gets()結束後就可以直接執行更長的ROPchain，我們就可以open, read, write了 ~

open, read, write

接下來就是要刻open, read, write：

1. open “/home/survey/flag”, return file fd
2. read file fd to buffer
3. write buffer to stdout

照著上課說的syscall表可以刻出來，詳細可參考程式碼： `code/Survey/exp.py`

Robot

解法

用gdb跟ida可以看出，這個程式碼的parent會跟child溝通，而其中的fd分別是：

- dprintf_read_fd = 0x3
- dprintf_write_fd = 0x4
- read_fd = 0x5
- write_fd = 0x6

有了fd後，就可以利用child寫shellcode跟parent溝通。

接下來要想辦法利用format string bug來打parent，先分析程式碼

剛開始有x, y, goal_x, goal_y四個座標，可以有以下三種操作：

1. S: 輸出當前位置，fmt = x + y + goal_x + goal_y，疑似主要漏洞，但限制太多
2. M: 移動上下左右（改變x, y），檢查可不可行，x跟y需在100內，並且fmt = Success或Failed
3. G: 放棄，疑似沒用

每次操作後goal_x, goal_y都會隨機減少0~1。

所以看起來只有S操作會回傳的四個字元可以來攻擊，但其中goal_x, goal_y又不是可以完全掌控，而且範圍又在100以內，沒辦法打n, p等字，而且總長度也只有4，感覺很難控，似乎有別種方法...

試著寫寫看shellcode，寫了一些迴圈來跟parent玩，可以做到控制x, y到想要的字元，將fmt控成 `%x..` 可以成功leak出stack上的東西，但似乎不是很有用...

解決長度只有4個字元的話，應該就可以利用rbp chain技巧來達到任意寫入，然後改return address或GOT等方法拿到shell。

（未拿到flag）

程式碼可參考： `code/Robot/exp.py`