Computer Security Homework 0x07

Real name: 涂世昱

Nick name: R07922115

Student ID: R07922115

Casino++

Introduction

這題跟`casino`唯一的差別在於它將`NX`的保護機制開啟了, 所以我們就不能把`shellcode`放在data段的某個地方然後在執行它, 所以就要用其他方式來得到它的`shell`。

我這邊用的方法是先將`libc`的位址在執行期間leak出來, 然後再將程式碼當中的某個`libc` function的`got`當中的位址改成`system`的位址, 並且將其參數想辦法改成`sh`就行了。

Walkthrough

casino forever

進入`casino function`之後, 我們可以用跟`0x05 (casino)`一樣的方法將`puts`的got改成`casino function`, 所以它最後就可以一直在`casino function`當中循環。

leak glibc address

為了將`libc`的位址leak出來, 我們必須要有可以輸出這個位址的function及其參數, 我這邊選擇是用`srand`, 我可以用同樣的方法將`srand@got`改為`printf@plt`的位置, 因為在程式碼當中`srand()`裡面的參數是傳入`seed`, 所以我們就必須把`seed`值改成某個`libc` function (我這邊用printf)的`got`位址, 預期它最終可以`printf(printf@got)`, 我就可以動態的leak出`printf@libc`。 為了改`seed`, 我就在程式的一開始在輸入`name`的時候將`seed` overflow成`printf@got (0x602030)`, 於是就成功得到了`printf@libc`的位址了。

change srand(seed) to system(sh)

leak出`printf@libc`之後, 我們可以用同樣的技倆將某個function的`got`改成`system@libc`, 這邊一樣是採用`srand`作為更改目標, 但為了將"sh"塞到`seed`裡面, 我在程式的一開始在輸入`name`的時候把"sh"蓋在`name`後面的某個地方(0x602110), 我們之後再把`seed`用`read_int()`的方式把它改成`0x602110`, 然後在循環回`casino()`, 再把`srand`(此時是printf), 改成`system`, 就可以成功執行`system(sh)`了。

wrappup

1. 在`main`輸入`name`時, 將`seed` overflow成`printf@got`, 再往後蓋到`0x602110`把"sh"蓋進去。
2. 進入`casino`將`puts@got`改為`casino`, 讓程式引發`puts`進而回到`casino`。
3. 將`srand@got`改成`printf@plt`, 跳到`casino`leak出`printf@libc`位址。
4. 將`seed`值改為`0x602110`, 跳回`casino`。
5. 計算出從`printf@libc`到`system@libc`的offset, `system@libc = printf@libc + offset`, 將`srand@got`改成`system@libc`, 跳回`casino`, get shell。