Computer Security Homework 0x05

Real name: 涂世昱

Nick name: R07922115

Student ID: R07922115

casino

Introduction

這題目的在於利用程式的漏洞, 更改`GOT`欄位所紀錄的位址, 又因為它沒開啟`NX`保護機制, 只要將shellcode塞到data段的某個地方, 然後將某個libc function的`GOT`欄位的位址指向它, 我們就可跳到那邊去執行shellcode, 就可以得到server的shell。

Walkthrough

在`main`當中題目要我們輸入`name`, 還有`age`, 進入`casino` function之後, 根據所輸入的name作為random seed, 然後隨機算出`lottery`, 接著再輸入`guess`, 輸入完之後問要不要換號碼, 選擇其中一個`guess`更換號碼, 而後開始比對`guess`和`lottery`的值是否相等, 一樣的話則`puts(''you win ...'')`, 然後再重複一次剛剛的輸入`guess`的過程, 離開迴圈之後就`printf(''you lose ...'')`。

Solution

在`main`會read 0x100個bytes, 可把shellcode塞到這裡面的其中一個地方, 因為shellcode太長的話會蓋到`age`變數, 輸入`age`之後shellcode就會無法執行, 所以不妨將shellcode塞到比較後面的地方, 我這邊所選的是`0x602120`, 然後在shellcode前面就任意填入'a'字元, shellcode的部份則是呼叫pwnlib的`asm(shellcraft.amd64.sh())`即可。

在`casino`當中可以利用`change number`的部份, 使用者可以更改`guess + idx`, `guess`的位置是在`0x6020d0`, `puts GOT`的位置是在`0x602020`, 我們可以相減算出兩者的距離, 然後轉成`int`傳進去`idx`, 然後把`guess + idx`所指到的位置的值改成某個位址, 就達成了可以成功hijack `puts GOT`。這邊因為`int`是4個bytes, `puts GOT`在load進來的值是`0x00007ffff7e2e080`, 我們要用`read_int()`的方式將它改為shellcode的位置(`0x602120`)顯然是要改兩次它才能成功, 而且不能改到一半, 呼叫這個libc function, 不然會無法執行就會離開了, 這邊所選擇的解法為第一次在填`guess`的時後故意塞錯的答案, 讓它不會`puts(''you win ...'')`, 更改`puts`的GOT, 然後第二次填入正確的`lottery`答案, 使它呼叫`puts`, 就可以成功跳到我們hijack的`puts GOT`, 成功執行我們的shellcode, 就可把flag cat出來了。

若選擇hijack printf, 則改了一半之後, 必定會call它, 一定不會順利執行。再來, 我們該如何猜正確的lottery答案呢, 因為一開始在輸入`name`的時候我們會將它在shellcode之前全都蓋'a', 連`seed`都蓋掉了, 所以用gdb看它每次`lottery`的值都是一樣的, 這樣一來就可以輸入正確的`guess`。