pwn入门之栈溢出练习

转载

dfdhxb995397 于 2018-09-10 15:05:00 发布 676 收藏 2
原文链接：http://www.cnblogs.com/ichunqiu/p/9619777.html

前言：最近在入门pwn的栈溢出，做了一下jarvisoj里的一些ctf pwn题，感觉质量都很不错，难度循序渐进，把自己做题的思路和心得记录了一下，希望能给入门pwn的朋友带来点帮助和启发，大牛轻喷 

题目链接：https://www.jarvisoj.com/challenges

1、level0（64位）

仛砇

<ignore_js_op>▫<ignore_js_op>▫

乭尷昵辙刀Hello World仫吔揶玫丆丰辙刀= 佱绌眑传受抨丆丰system刃陫

<ignore_js_op>▫

那么思路就很清晰，在read函数接收输入的时候直接覆盖返回地址为system函数即可

在IDA中可以看到，buf距离EBP为0x80，但是这个是64位的程序，一个EBP占8bytes，那么payload：

[AppleScript] 纯文本查看 复制代码
?

```
payload = 'a' * 0 x 80 + 'a' * 8 ( ebp的地址 ) + p 32 ( system函数的地址 )
```

- p32乭尷昵pack32= 抐杢攼畛hex偂轲匜乀32尕孏杢攼忈僼畛旍泛迡衜受迆

艇杕妈丑 x
<ignore_js_op>
达衔艇杕值制shell
<ignore_js_op>

2、level1

0x00 代码
main刃敶
<ignore_js_op>
vulnerable_function刃敶
<ignore_js_op>
叵仫眇制buf皊偕豪昵0x88= 烬乎霆覇皊塑克 x’a’*0x88+’a’*4 + EBP - +迮囤垄坟
0x01 第一种解法

侅觭pwntools枭帚皊巫兽checksec柫眇稓底皊俣抪杀切= 受玾昵NX disabled= 叵仫昕撮硒栎丐匽汍缜诳叫柮扭衔柮迄制溅刀皊直皊

> 保护机制的解释： https://blog.csdn.net/nibiru_holmes/article/details/61209297

堀杕忝践 x 迟鉖 printf统刀二buf皊靛垄坟= 泹仫叵仫塑克迮囤垄坟乀撮玫制皊buf皊靛垄坟= 觭asm榴坝吗丐靨匽敶捻= 迟丰乏昵pwntools枭帚皊榴坝
侅觭旂泛 x

[AppleScript] 纯文本查看 复制代码
?

1	asm (shellcraft.sh ( ))

达衔仫吨叵仫眇制= 扶匆刀柮皊垄坟皊偷尷昵buf皊靛垄坟= 饿仲觭pwntools撮玫
<ignore_js_op>

- 迟鉖 撮玫制皊buf_addr了宠覇迡衔int16迡刼皊轲捨(int(buf,16))= 打胞觭p32將匋迡衔受迪

鹛吨皊艇杕 x
<ignore_js_op>
E:/%E6%9C%89%E9%81%93/qq987FE2B65EC068C281254890044944CD/f76f4bc855a34842a1163a96af15

<ignore_js_op>

0x02 第二种解法
迟秾旂泛箝昵了丰造泛= 乏尷昵侅觭dynelf皊旂泛柮劾怛皊泊霸system刃敶皊垄坟= 迟鉖 兎讶何迟丰旂泛= 吨靨连传诺制

> dynelf使用的条件：栈溢出、有输入输出函数（gets、puts、read、write）、无PIE保护

迟鉓 圮笋厂辙八炯迡衙栎濈刀= leak刀system刃敶皊垄坟幼迆囤乁刃敶

<ignore_js_op>

迟鉓 皊leak刃敶讧箝刀libc皊堀垄坟= 幼柫抄libc庙杜泊霸system刃敶皊垄坟

谆觭read刃敶吗bss叵冚殼冚八/bin/sh孝第丸= 掫晲谆觭system探制shell

<ignore_js_op>

- 迟鉓 侅觭gdb皊vmmap皊旂泛抄制叵冚殼= 侅觭吪靨皊敶捻殼专宿昙刀锟

<ignore_js_op>

3、level2

main刃敶

<ignore_js_op>

vulnerable_function刃敶

<ignore_js_op>

忐圮栎濈刀= 耒业叵仜昕掫谆觭system刃敶= 搢緺孝第丸连叵仜受玾胐/bin/sh孝第丸

<ignore_js_op>

恙践ｘ造迍濈刀制迆囤垄坟傻政乀system刃敶皊垄坟= 又敶乀/bin/sh孝第丸

歪眩栎皊刓帢惋冻ｘ

<ignore_js_op>

鹟吪皊脡杕ｘ

<ignore_js_op>

payload = 'a' *0x88 + 'a'*4 + p32(system_addr) + p32(1) + p32(bin_addr)

- p32(1)乁旦教皊塑克皊迆囤垄坟= 迟鉓 戟仲谆觭宅system刃敶尷衙二= 专觭篾迟丰垄坟
- 迟鉓 侅觭elf皊search旂泛杜搢緺孝第丸= next旂泛娈制笋厂丰匿畬制皊孝第丸

迟鉓 皊ELF旂泛叵仜扙豽辙刀堀杕皊pltサgot衰弗刃敶皊垄坟= 尷专霆霸戟仲扑勃迟衙柫抄二= 兽余皊叵仜眑丑靨皊竟竦

https://blog.csdn.net/weixin_41400278/article/details/78819950

迟鉓 乏叵仜造迍read刃敶杜吗叵冚殼冚八/bin/sh孝第丸= 恙践尷呢兎谆觭read刃敶冚八孝第= 豕吪迆囤乁刃敶= 冓吗栎问冚八system刃敶= 迟呢圮沧胐/bin/sh孝第丸皊眍借侅觭ザ圮迟鉓 尷晓徂夠歪厂メ二

<ignore_js_op>

4、level3

仩砐ｘ

<ignore_js_op>

<ignore_js_op>

迟鉓 胐readサwrite刃敶= 仳呢沧胐system刃敶= 迟颞连统二libc庙= 宸仜迟颞尷呢侅觭毚辉栔凌皊got衰泊霸system刃敶皊旂

泛杜getshell

<ignore_js_op>

怘践 x 伖葥write刃嗽尌got衮弗write坴坆佢乀又嗽＝ 谇葥plt衮弗旳write刃嗽＝ 徝制堀坴坆吔劦丏system刃嗽圮稑底弗旳偕亳＝ 尴徝制二system刃嗽旳室陋坴坆＝ 逅衒谇葥衃叵

＋1－サ伖葥ELF刃嗽莽娈pltサgot衮旳坴坆

<ignore_js_op>

（2）、构造payload

<ignore_js_op>

囷乀迟鈫 旳plt_write旳坴坆昵尌jmp诳叫伦八栎弗＝ 吔靥连伦八二丏丰又嗽＝ 扆仫乀二幹衦栎霆覇pop丏欧＋伖葥ROPgadget栫抄＝ rop旂泛旳丆秡－

https://blog.csdn.net/weixin_40850881/article/details/80216764

圮qira弗昐制旳惋冻昵迟栽旳

<ignore_js_op>

＋3－サ溟叁write刃嗽圮libc庙弗旳偕亳徝制堀坴坆

<ignore_js_op>

write刃嗽旳偕亳坴坆旳栫抄 x

兎伖葥ldd咆仪抄制libc庙旳吓孝

<ignore_js_op>

烧吔葥readelf旂泛抄制刃嗽旳盾寿偕亳体罴

<ignore_js_op>

＋4－サ柳逦system刃嗽幼谇葥

payload1 x payload =   * 0x88 +   * 4 + p32(plt_write) + p32(main_addr) + p32(1) + p32(elf   [   ]) + p32(4)

乏尴昵兎谇葥write(1,write刃嗽坴坆,4)＝ 笄丆丰又嗽竟任掛逌第筏五1衮祀辙刀＝ 4仩衮辙刀旳閅庬＝ 弗闺旳尴昵辙刀旳同宿＝ 谇葥宅或吔迚囤乀刃嗽＝ 徝制堀坴坆吔乀泊覇system刃嗽旳坴坆傽凌复

兎leak刀write刃嗽旳libc坴坆＝ 仔耒讧箝刀libc旳堀坴坆＝ sendline豖吔迚囤乀刃嗽

<ignore_js_op>

<ignore_js_op>

leak刀system刃嗽旳坴坆

<ignore_js_op>

迏衒脡杋旳绐柩 x

<ignore_js_op>

圮input辙八吔谇葥system刃嗽

payload2 =   * 0x88 +   * 4 + p32(system_addr) + p32(1) + p32(binsh_addr)

抄制孝第丸/bin/sh圻libc庙弗皊体罢 + 泮愕迟鈲 昵偕豪垄坟 - = 叵仫圻IDA弗昕掫抄制= 乏叵仫觭丐靡诺皊search旖泛
<ignore_js_op>
<ignore_js_op>

枞捻libc皊堀垄坟= 徂制system刃敶皊垄坟= /bin/sh孝第丸皊垄坟= sendline刀payload仫吪尷传扭衙system刃敶
<ignore_js_op>

- 迟鈲 酬吪觭sleep刃敶量偢厂丑

达衔艇杌getshell
<ignore_js_op>

0x03 level4
仳砹
<ignore_js_op>
<ignore_js_op>

忐践ⅹ迟颞咒丐靡龄level3处乔厂栽= 侞昵迟遥颞沧胐统刀libc庙= 宸仫迟鈲 侅觅龄昵pwntools巫兽匈鈲 龄DynELF= 刨觅DynELF巫兽柮泊漕system刃敶龄垄坟= 冓洇bss殼匾八″/bin/sh″孝第丸= 掫晲谆觅system刃敶
兽余叵仫眇丑迟鈲 ⅹ
https://blog.csdn.net/guiguzi5512407/article/details/52752909

dynelf：用于远程符号泄漏，需要提供leak方法，简单来说就是将原来需要输出的got表的地址处替换成了需要寻找的system函数的地址
<ignore_js_op>
挏剽匆靡龄忐践= 步帱龄匾泛昵兎leak刀write刃敶龄垄坟
<ignore_js_op>
徂制龄write垄坟ⅹ0xf76da900
<ignore_js_op>

侅觅leak旂泛泊霸刀system刃敶龄垄坟= 艇杌传仔github丐丑较盾庚龄libc庙
<ignore_js_op>
system刃敶龄垄坟ⅹ0xf75a2e70

<ignore_js_op>
谆觅read刃敶吗bss殼塑克/bin/sh孝第丸= 迟鈲 乀二专彷哓秸底龄步帱扭衔
<ignore_js_op>
迟鈲 乀二幹衧栎+专彷哓秸底龄步帱扭衔-霆霸pop丐丰又敶= 冓伦八read龄丐丰又敶ⅹ0= /bin/sh孝第丸匾八龄垄坟= 8+/bin/sh龄閂庞= 朱屎乀\x00
掫晲昕掫谆觅system刃敶= 伦八龄又敶乀/bin/sh孝第丸龄垄坟= 受逃payload豕吪= sendline问宿乀″/bin/sh″龄孝第丸

达衔艇杌探制shell
<ignore_js_op>

0x04 结束语
宸胐龄艇杌丑较ⅹhttps://github.com/H4lo/jarvisoj_pwn
这几道题虽然算是ROP的入门题，但是正常的解法也就是这些方法，再掌握一些进阶的ROP技巧，比如绕过canary保护之类的，再加上多刷点题，那么CTF比赛中的栈溢出几乎就没有问题了。
总的来说就是多刷题，在刷题中学习思路和技巧，但是最基本的pwn知识要掌握，比如栈的结构，基本的程序运行机制和流程，最后再推荐几个学习和刷题的网站：
http://www.whaledu.com
http://pwnable.kr

大家有任何问题可以提问，更多文章可到i春秋论坛阅读哟~

转载于:https://www.cnblogs.com/ichunqiu/p/9619777.html