[hw0x01] writeup

莊翔旭, woolninesun, b04902083

short_shell

觀察到 read 只能讀 10 bytes, 且最後會跳到 buffer 上跑，在 call buffer 之前設置 eax = 0x0, edi = 0x7b, rsi 和 rdx 都指向 buffer。
第一次先改變 read 的 byte 數量，構造 syscall read(rdi = 0, rsi, rdx = 0x7b) + call rsi，剛好 10 bytes。
第二次改變 read 的 buffer，構造 syscall read(rdi = 0, rsi = rsp, rdx = 0x7b) + call rsp。
這樣就可以把 execve /bin/sh 的 shellcode 丟進 stack 然後執行！

shellsort2.0 （未解出）

看到題目 sort 猜測和 sort 有關，開 gdb 測試後發現會將丟進去的資料以 byte 為單位由大排到小，然後在 sort 完之後會把 esi, edi, eax 設成 0，在跳到 sort 過的 buffer 上執行。

嘗試組出 sort 過後還可以執行的 shellcode，有發現 syscall sort 過後都在後面不會移動，想試著組出 read 或直接 execve，不過都失敗...