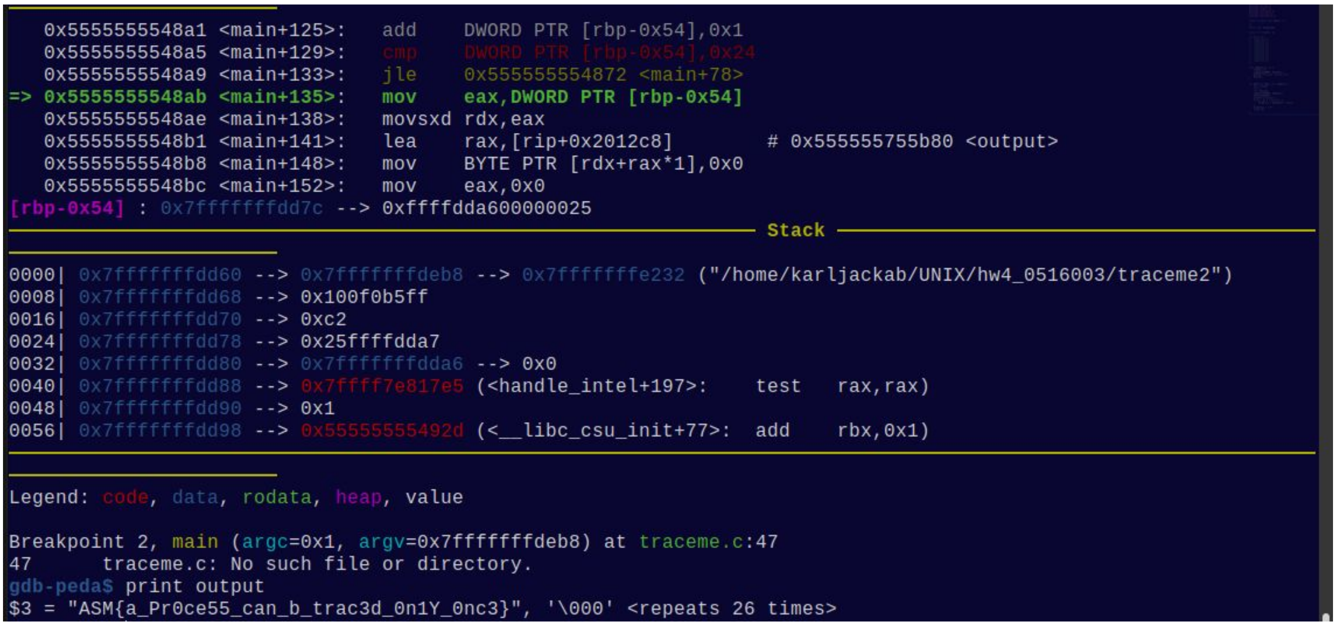
UNIX hw4

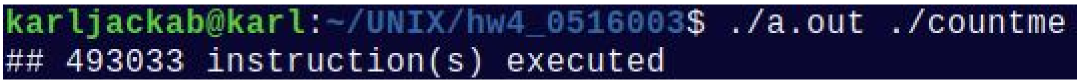
0516003 李智嘉

- traceme
  1. 利用gdb去trace traceme2
  2. 設定break point在line 47
  3. 利用continue執行到第47行
  4. 將output print出來，得到flag



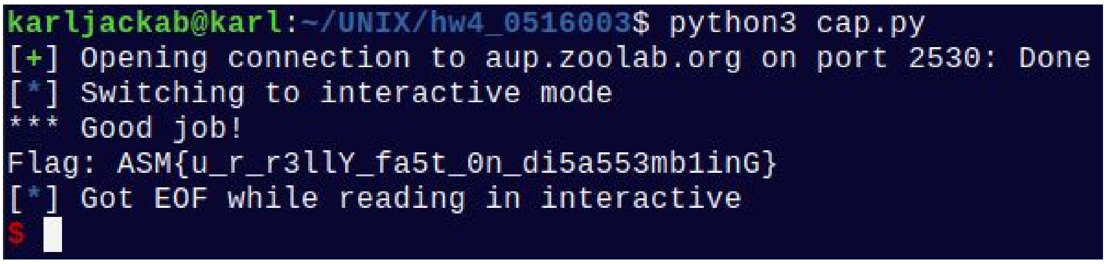
```
   0x5555555548a1 <main+125>:   add    DWORD PTR [rbp-0x54],0x1
   0x5555555548a5 <main+129>:   cmp    DWORD PTR [rbp-0x54],0x24
   0x5555555548a9 <main+133>:   jle    0x555555554872 <main+78>
=> 0x5555555548ab <main+135>:   mov    eax,DWORD PTR [rbp-0x54]
   0x5555555548ae <main+138>:   movsxd rdx,eax
   0x5555555548b1 <main+141>:   lea    rax,[rip+0x2012c8]        # 0x555555755b80 <output>
   0x5555555548b8 <main+148>:   mov    BYTE PTR [rdx+rax*1],0x0
   0x5555555548bc <main+152>:   mov    eax,0x0
[rbp-0x54] : 0x7fffffffdd7c --> 0xffffdda600000025
                                                                  Stack

0000| 0x7fffffffdd60 --> 0x7fffffffdeb8 --> 0x7fffffffe232 ("/home/karljackab/UNIX/hw4_0516003/traceme2")
0008| 0x7fffffffdd68 --> 0x100f0b5ff
0016| 0x7fffffffdd70 --> 0xc2
0024| 0x7fffffffdd78 --> 0x25ffffdda7
0032| 0x7fffffffdd80 --> 0x7fffffffdda6 --> 0x0
0040| 0x7fffffffdd88 --> 0x7ffff7e817e5 (<handle_intel+197>:    test   rax,rax)
0048| 0x7fffffffdd90 --> 0x1
0056| 0x7fffffffdd98 --> 0x55555555492d (<__libc_csu_init+77>:  add    rbx,0x1)

Legend: code, data, rodata, heap, value

Breakpoint 2, main (argc=0x1, argv=0x7fffffffdeb8) at traceme.c:47
47      traceme.c: No such file or directory.
gdb-peda$ print output
$3 = "ASM{a_Pr0ce55_can_b_trac3d_0n1Y_0nc3}", '\000' <repeats 26 times>
```

- countme
  1. 直接使用範例程式 “counter.c”，計算countme instructions 數



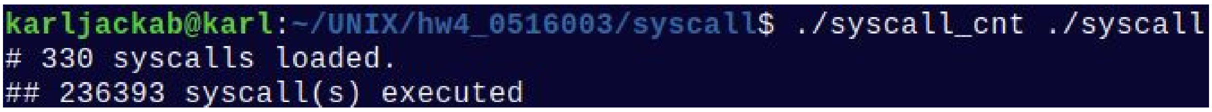
```
karljackab@karl:~/UNIX/hw4_0516003$ ./a.out ./countme
## 493033 instruction(s) executed
```

- capstone



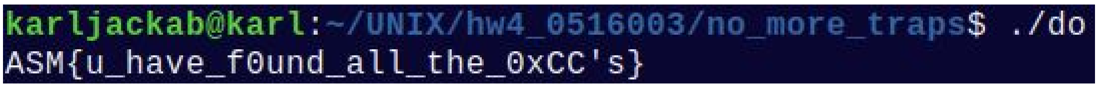
```
karljackab@karl:~/UNIX/hw4_0516003$ python3 cap.py
[+] Opening connection to aup.zoolab.org on port 2530: Done
[*] Switching to interactive mode
*** Good job!
Flag: ASM{u_r_r3llY_fa5t_0n_di5a553mb1inG}
[*] Got EOF while reading in interactive
$
```

- syscall
  1. 修改範例程式，套用到題目的程式上，就可以計算出 syscalls 數量



```
karljackab@karl:~/UNIX/hw4_0516003/syscall$ ./syscall_cnt ./syscall
# 330 syscalls loaded.
## 236393 syscall(s) executed
```

- no more traps
  1. 修改範例程式autodbg.cpp，並將題目提供的 opcodes 套到程式裡面，即可得到flag



```
karljackab@karl:~/UNIX/hw4_0516003/no_more_traps$ ./do
ASM{u_have_f0und_all_the_0xCC's}
```