HSGS Sec Day 05

Quiz and Homework

Quiz

Mã hàm của syscall nằm ở thanh ghi nào?

- RDI
- RAX
- RSI
- R10

Mã hàm của syscall nằm ở thanh ghi nào?

- RDI
- RAX
- RSI
- R10

Mã hàm của syscall exit?

- 0
- 60
- 1
- 2
- 3

Mã hàm của syscall exit?

- 0
- 60
- 1
- 2
- 3

data khởi tạo bằng 0 sẽ được chứa ở section nào?

- .text
- .bss
- .data
- .rodata

data khởi tạo bằng 0 sẽ được chứa ở section nào?

- .text
- .bss
- .data
- .rodata

Chương trình Assembly sau sẽ? (chọn tất cả các phương án đúng)

- Không biên dịch được
- Kết thúc bình thường (exit 0)
- SIGSEGV (Segmentation fault)
- Đọc input và kết thúc
- In "Hello World" và xuống dòng
- Tất cả các phương án còn lại đều sai

```
1   section .text
2   global _start
3   _start:
4       mov rcx, .end
5
6       mov rdi, 0
7       mov rsi, s
8       mov rdx, s.end - s
9       mov rax, 0
10      syscall
11      jmp rcx
12  .end:
13      xor rdi, rdi
14      mov rax, 60
15      syscall
16      hlt
17  section .data
18  s:
19      db "Hello World", 0xa
20  .end:
```

Chương trình Assembly sau sẽ? (chọn tất cả các phương án đúng)

- Không biên dịch được
- Kết thúc bình thường (exit 0)
- SIGSEGV (Segmentation fault)
- Đọc input và kết thúc
- In "Hello World" và xuống dòng
- Tất cả các phương án còn lại đều sai

```
1   section .text
2   global _start
3   _start:
4       mov rcx, .end
5
6       mov rdi, 0
7       mov rsi, s
8       mov rdx, s.end - s
9       mov rax, 0
10      syscall
11      jmp rcx
12  .end:
13      xor rdi, rdi
14      mov rax, 60
15      syscall
16      hlt
17  section .data
18  s:
19      db "Hello World", 0xa
20  .end:
```

Takeaways

- SYS_READ = 0; SYS_WRITE = 1
- stdin: 0; stdout: 1; stderr: 2
- SYSCALL thay đổi RAX, RCX và R11
  - RAX là giá trị trả về
  - RCX là địa chỉ code thực hiện khi trả về
  - R11 là rflags khi trả về
- Learn how to use a debugger, not just debug printing

Command để compile file code.s thành code

- nasm -f elf64 -g -o code.o code.s; ld -static -o code code.o
- nasm -f elf64 -g -o code code.s
- ld -static -o a a.o
- Không phải 3 phương án trên

Questions for quiz?

Homework

P33014

- In ra 100 dòng “Chau Bac Ho”

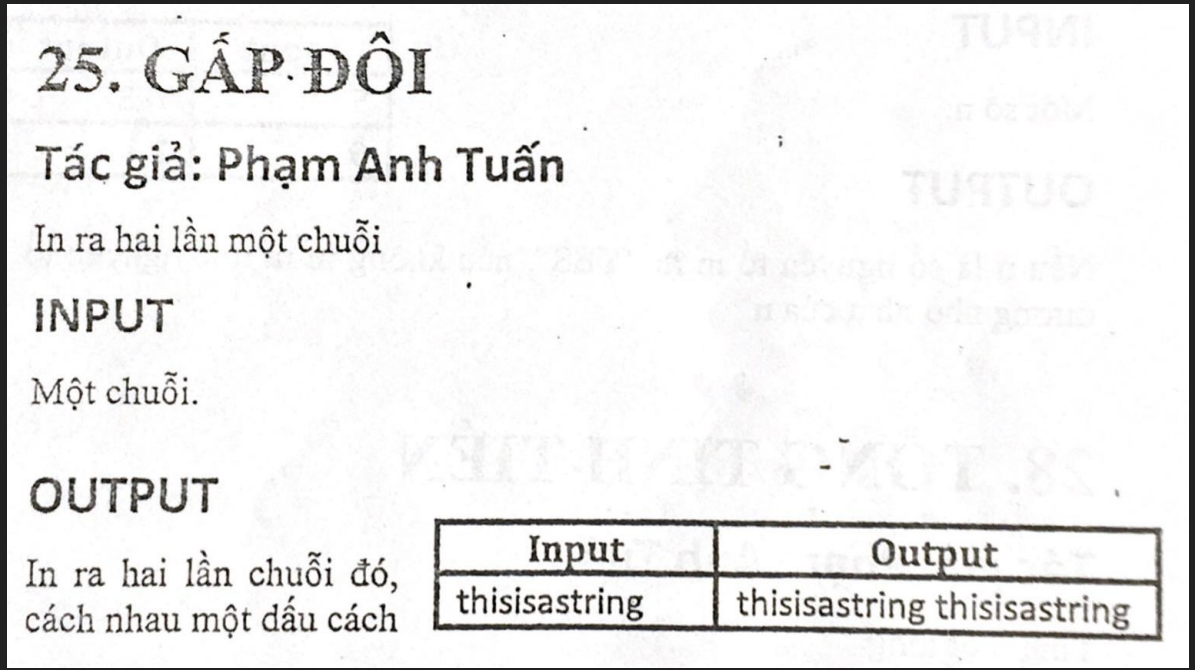
P33014

- In ra 100 dòng “Chau Bac Ho”

```
section .text
global _start
%define SYS_EXIT 60
%define SYS_READ 0
%define SYS_WRITE 1

_start:
    mov r12, 100
.L1:
    mov rdi, 1
    mov rsi, s
    mov rdx, s.end - s
    mov rax, SYS_WRITE
    syscall

    dec r12
    cmp r12, 0
    jg .L1

    xor rdi, rdi
    mov rax, SYS_EXIT
    syscall
    hlt

section .data
s:
db "Chau Bac Ho", 0xa
.end:
```

P025

- Gợi ý: có thể check các kí tự ‘ ‘ (0x20); ‘\n’ (0xa); 0x0; read fail để tìm bắt đầu và kết thúc của xâu.



25. GẤP ĐÔI

Tác giả: Phạm Anh Tuấn

In ra hai lần một chuỗi

INPUT

Một chuỗi.

OUTPUT

In ra hai lần chuỗi đó, cách nhau một dấu cách

Input	Output
thisisastring	thisisastring thisisastring

P025 - kjudge

- Test easy

```
12  global _start
13  _start:
14      xor rdi, rdi
15      mov rsi, s
16      mov rdx, s.end - s
17      mov rax, SYS_READ
18      syscall
19
20      mov qword [n], rax
21      mov rsi, s
22      mov rdx, rax
23      inc rdx
24      mov byte [rsi + rax], 0x20 ; ' '
25      mov rdi, 1
26      mov rax, SYS_WRITE
27      syscall
28
29      mov rsi, s
30      mov rdx, qword [n]
31      mov rdi, 1
32      mov rax, SYS_WRITE
33      syscall
```

```
34
35      xor rdi, rdi
36      mov rax, SYS_EXIT
37      syscall
38      hlt
39
40  section .bss
41  n:
42      resq 1
43  s:
44      resb 0x100
45  .end:
```

P025 - Codefun

- Input bẩn
- Test có thể có thừa dấu cách/xuống dòng ở đầu/cuối
- Cần tìm điểm bắt đầu và kết thúc của xâu

P025 - Codefun

```
1   section .text
2   %define SYS_READ 0
3   %define SYS_WRITE 1
4   %define SYS_EXIT 60
5   global _start
6   _start:
7       xor rdi, rdi
8       mov rsi, s
9       mov rdx, s.end - s
10      mov rax, SYS_READ
11      syscall                 ; read all input
12
```

P0

```
12
13      mov rdi, s              ; rdi = s
14      add rax, rdi            ; rax = ptr to input's end
15      mov dl, 0               ; found string?
16  .L1:
17      cmp rdi, rax            ; for(char *rdi = s; rdi < rax; rdi++) {
18      jge .end
19      mov cl, byte [rdi]      ; char c = *rdi;
20      inc rdi                 ; rdi++;
21      cmp cl, 0x21 ; '!'      ; if (c < '!'
22      jl .invalid
23      cmp cl, 0x7e ; '~'      ;     || c > '~') goto .invalid;
24      jg .invalid
25      cmp dl, 1               ; if (dl == 0) {
26      je .L1
27      mov dl, 1               ;   dl = 1;
28      lea rsi, [rdi - 1]      ;   rsi = rdi - 1; // string start
29      jmp .L1                 ; }
30                              ; }
31  .invalid:
32      cmp dl, 1               ; if (dl != 1) continue; not found string yet
33      jne .L1
34      dec rdi                 ; rdi -= 1;
35  .end:
36      ; rdi: string end
37      ; rsi: string start
```

P025

```
35  .end:
36      ; rdi: string end
37      ; rsi: string start
38      mov rdx, rdi
39      sub rdx, rsi            ; rdx: string length
40      mov qword [a] , rsi     ; save string start
41      mov qword [n], rdx      ; save string length
42      mov byte [rdi], 0x20    ; ' ' : set last char to space
43      inc rdx                 ; write 1 more (space)
44      mov rdi, 1
45      mov rax, SYS_WRITE
46      syscall
47
48      mov rsi, qword [a]
49      mov rdx, qword [n]
50      mov rdi, 1
51      mov rax, SYS_WRITE
52      syscall
53
54      xor rdi, rdi
55      mov rax, SYS_EXIT
56      syscall
57      hlt
58
```

```
58
59  section .bss
60  a:
61      resq 1
62  n:
63      resq 1
64  s:
65      resb 0x100
66  .end:
```

P032

32. CHUỖI THẦN KỲ

Tác giả: Phạm Anh Tuấn

Nhập vào một chuỗi. In ra màn hình theo mẫu sau:

Input	Output
string	s
	st
	str
	stri
	strin
	string
	string
	strin
	stri
	str
	st
	s

33. PHÉP CHIA

Tác giả: Phạm Anh Tuấn

P032

- Đọc input
  - Kjudge: simple read
  - Codefun: P025
- 2 vòng for: 1 xuôi 1 ngược để in xâu
  - Lưu độ dài, biến đếm xâu ra .bss

Questions on Homework?