Task 1: output

str: 0x400600 pos: 0x400607 T

TASK 2: cat main.S

.file "main.c"

.section .rodata

.LC0:

.string "String Tested"

.LC1:

.string "str: %p pos: %p %c \n"

.text

.globl main

.type main, @function

main:

.LFB0:

.cfi\_startproc

pushq %rbp

.cfi\_def\_cfa\_offset 16

.cfi\_offset 6, -16

movq %rsp, %rbp

.cfi\_def\_cfa\_register 6

subq $16, %rsp

movq $.LC0, -8(%rbp)

movq -8(%rbp), %rax

#APP

# 5 "main.c" 1

cld

movq %rax, %rdi

movb $84, %al

repne scasb

decq %rdi

movq %rdi, %rax

# 0 "" 2

#NO\_APP

movq %rax, -16(%rbp)

movq -16(%rbp), %rax

movzbl (%rax), %eax

movsbl %al, %ecx

movq -16(%rbp), %rdx

movq -8(%rbp), %rax

movq %rax, %rsi

movl $.LC1, %edi

movl $0, %eax

call printf

leave

.cfi\_def\_cfa 7, 8

ret

.cfi\_endproc

.LFE0:

.size main, .-main

.ident "GCC: (GNU) 4.8.5 20150623 (Red Hat 4.8.5-28)"

.section .note.GNU-stack,"",@progbits

Task 3: output

msr: f7ce43

Task 4: c source

#include <stdio.h>

#include <stdint.h>

int main() {

uint64\_t c = 0, b = 1000, a = 2000;

asm("lea 10(%1, %2, 4), %0\n"

: "=r"(c)

: "r"(b),"r"(a)

);

printf ("c=%lld", c);

}

ASSEMBLY

.file "main.c"

.section .rodata

.LC0:

.string "c=%lld"

.text

.globl main

.type main, @function

main:

.LFB0:

.cfi\_startproc

pushq %rbp

.cfi\_def\_cfa\_offset 16

.cfi\_offset 6, -16

movq %rsp, %rbp

.cfi\_def\_cfa\_register 6

subq $32, %rsp

movq $0, -8(%rbp)

movq $1000, -16(%rbp)

movq $2000, -24(%rbp)

movq -16(%rbp), %rax

movq -24(%rbp), %rdx

#APP

# 5 "main.c" 1

lea 10(%rax, %rdx, 4), %rax

# 0 "" 2

#NO\_APP

movq %rax, -8(%rbp)

movq -8(%rbp), %rax

movq %rax, %rsi

movl $.LC0, %edi

movl $0, %eax

call printf

leave

.cfi\_def\_cfa 7, 8

ret

.cfi\_endproc

.LFE0:

.size main, .-main

.ident "GCC: (GNU) 4.8.5 20150623 (Red Hat 4.8.5-28)"

.section .note.GNU-stack,"",@progbits

OUTPUT

c=9010