IC221 Lab: Makefiles and Debugging Name: FRANCESCONI

Worksheet / Gradesheet AY22S, 95 points total

Part 1 Gradesheet

(15) Task 1 -- Simple compilation makefile:

(30) Task 2 -- Multi-part makefile:

Part 2 Worksheet / Gradesheet

(10) A loop is often identified with an increment of a variable value by one (0x1) using the add instruction. There are two loops in the program. Identify an example of this kind of increment-by-one instruction in each loop, and copy the examples into your worksheet.

|  |
| --- |
| 0x00000000000011d7 <+142>: add DWORD PTR [rbp-0x54],0x1  0x0000000000001200 <+183>: add DWORD PTR [rbp-0x54],0x1 |

(10) Give one example of an assembly instruction from main() that assigns a local variable its value using the mov instruction, which copies a value to memory.

|  |
| --- |
| 0x0000000000001164 <+27>: mov DWORD PTR [rbp-0x50],0xb1 |

info locals

(10) What are the local variable names?

|  |
| --- |
| Name Current Value  i = 0  s1 = "UU\000\000\340\340\377\377\377\177\000"  s2 = {-8176, 32767, -7351, 32767, -134408736, 32767, 1431655037, 21845, -134503704, 32767, 1431654960, 21845} |

(10) Now that s1 is not obfuscated, what is its secret value?

|  |
| --- |
| s1 = "NINETYTWO!!\377" |

(10) Looking at the source code, describe the means by which the string is obfuscated:

|  |
| --- |
| All of the bits at each index in s1 are set equal to the inversion of the bits in s2 the first loop and masked. This results in the secret message in s1. The message is obfuscated when the values are masked again in the second loop. |