**CYB 220 Lab 6 - Binary Analysis Lab (Nov 1, 2024)**

**Due**: Friday, Nov 8, 2024, 11:59 pm.

**Turn in**: This report

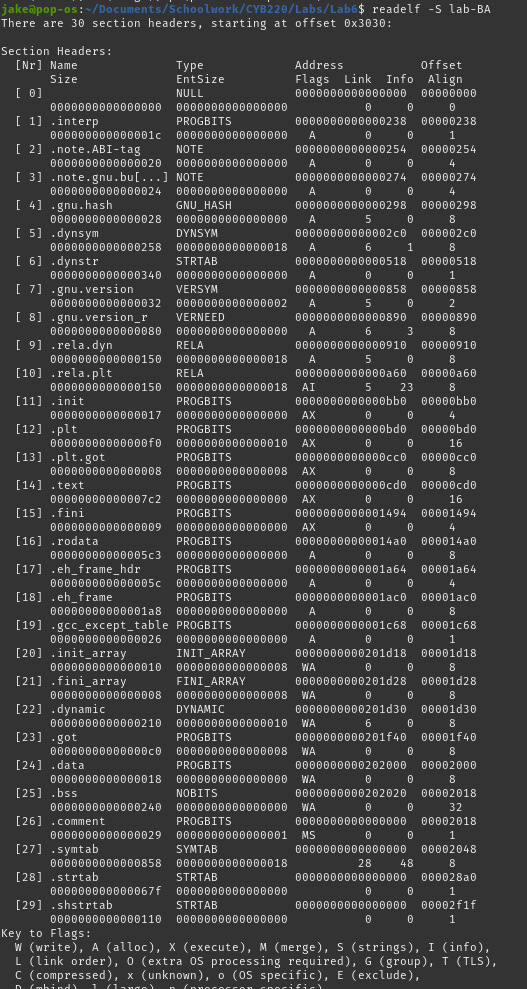
Points: 30 pts

**Objective**: Play with a binary executable (compressed in Lab-Binary.tgz) and learn how to use readelf, objdump utilities.

Name: Jake Gendreau

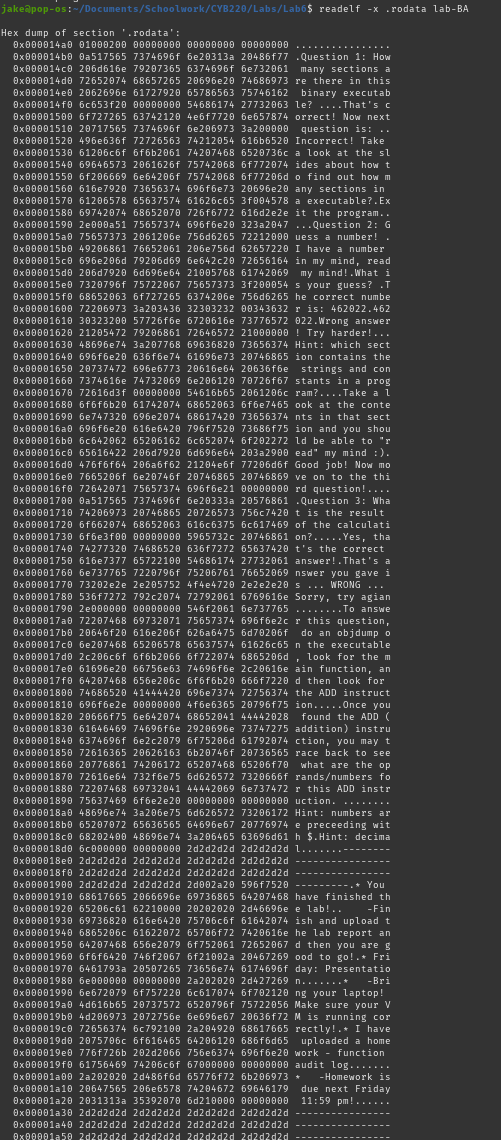
(5 pts)Question 1: How many sections are there in this binary executable?

Take a screenshot of the command you were using and the result from the command where you get your answer. Briefly explain.

I used readelf -S lab-BA to read all of the section headers of the file. These are conveniently numbered, revealing that there are 30 sections.

(10 pts)Question 2: Which section stores the constants and strings in a binary executable? Find the answer from that section.

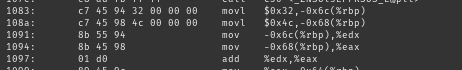
Take a screenshot of the command and the result where you found the answer to this question.



The answer to this question was revealed using the readelf -x .rodata command. The rodata section is short for "read-only data", which includes strings and constants. Doing a hexdump with -x reveals all of the strings and constant values in the program.

(10 pts)Question 3: What is the result of the arithmetic calculation?

Take a screenshot of the relevant part of the assembly code, and explain how you figured out the correct answer.

Using objdump -d to disassemble the file, I searched through the file for main, then used grep to look for all instances of add. I found that operation 1097 was an add operation, and was also in the main section. Looking at the preceding code, I found that 0x32 was loaded into the higher bits of rbp, and that 0x4c was loaded into the lower bits of rbp. They are then moved to edx and eax, then when added, the result is 126.

(5 pts)Take a screenshot when you correctly answer all 3 questions.

[paste here]

