CSC 472 Fall 2024 Lab 1

Dr. Si Chen

September 11, 2024

Introduction

The goals of this lab are:

- Understanding the concepts of stack and stack frames in C programming.
- Using GDB to reverse engineer and read the assembly code.

Our course webpage: https://www.cs.wcupa.edu/schen/ss2024/

Lab Instructions

Step 1: Connect to the CTF System

Connect to the badger CTF system and navigate to the folder `lab1`.

```
cd ss2024/lab1
```

Step 2: Use GDB to Analyze the Binary Program

```
gdb lab1
```

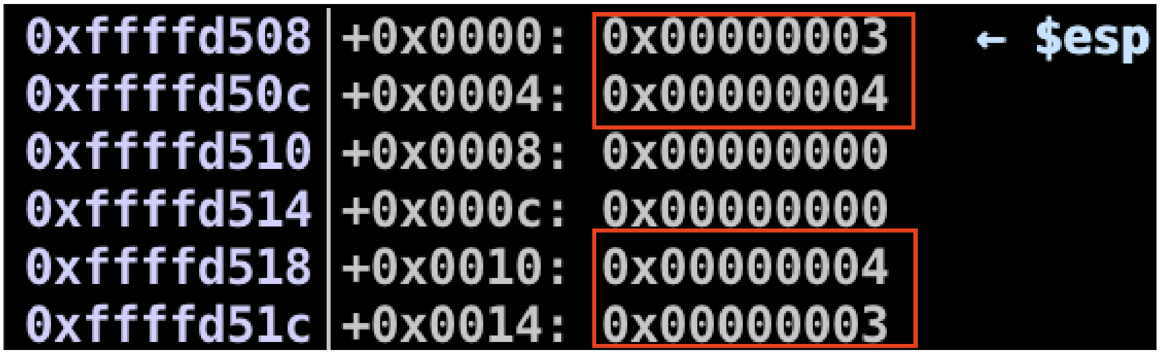
Step 3: Disassemble the `main` Function

```
disas main
```

Questions:

1. Q1: Identify the assembly instructions for creating the stack frame of the `main()` function. (1 point)
2. Q2: Identify and explain the purpose of the two lines related to setting variables `p` and `q`. (1 point)

3. Q3: Before calling `multiply_by_two()`, why does the stack contain two sets of “3,4” instead of just one set (see Figure.1)? (1 point)



```
0xffffd508│+0x0000: 0x00000003    ← $esp
0xffffd50c│+0x0004: 0x00000004
0xffffd510│+0x0008: 0x00000000
0xffffd514│+0x000c: 0x00000000
0xffffd518│+0x0010: 0x00000004
0xffffd51c│+0x0014: 0x00000003
```

Figure 1: Two sets of “3,4”

Step 4: Disassemble the `multiply_by_two` Function

```
disas multiply_by_two
```

Questions:

1. Q4: Explain the meaning of `add eax,edx` and `add eax,eax`. Why not using mul (Multiply) instruction instead (take a guess)? (1 point)
2. Q5: Which register is used to store the final multiplication result? (1 point)

Deliverables

Submit a detailed project report in PDF format to answer the above questions. Include pictures, diagrams, and code snippets.

Submission

- Check the lab due date on the course website. Late submissions will not be accepted.
- Submit your assignment to D2L directly.
- **No copy or cheating is tolerated**. If your work is based on others’, please give clear attribution. Otherwise, you **WILL FAIL** this course.