Introduction to Cybersecurity
CS/IS 193

LAB15 REPORT

5/29/2022

DAVID ARCHER

Table of Contents

1. **Introduction** **3**
2. **Lab Results** **3**

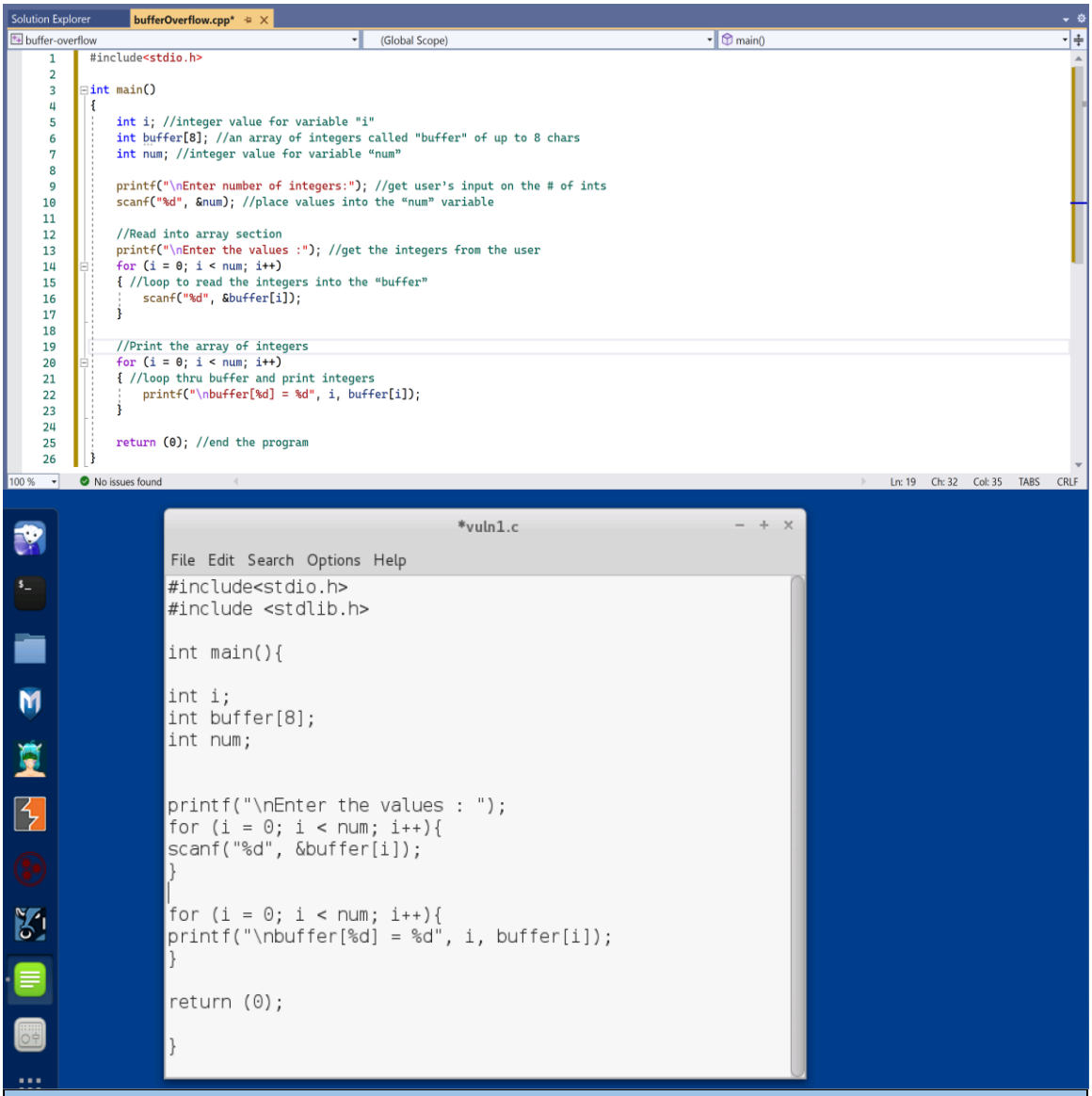
1. Introduction

In this lab I will write a buffer overflow program, run code to demonstrate buffer overflow, analyze and modify overflow code.

2. Lab Results

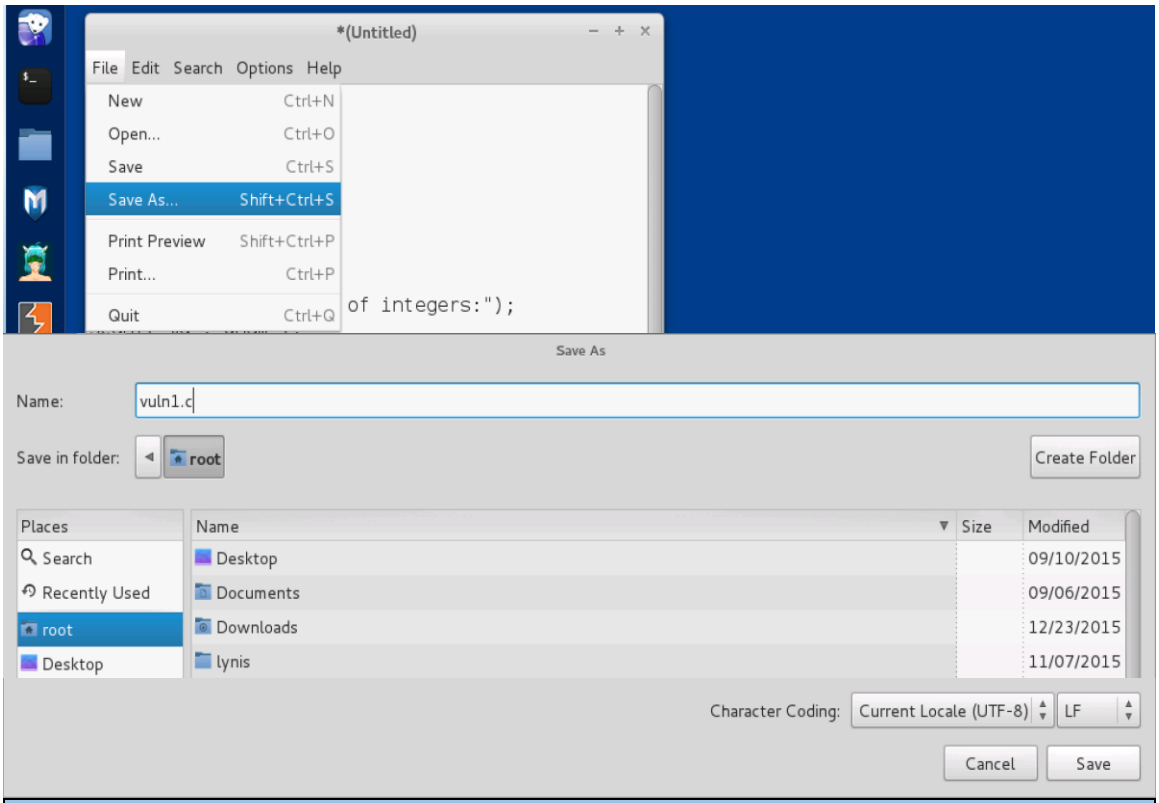
1. Writing a Buffer Overflow Program

1. Kali Linux VM Leafpad editor



Within the leafpad editor, inputted a script written in C.

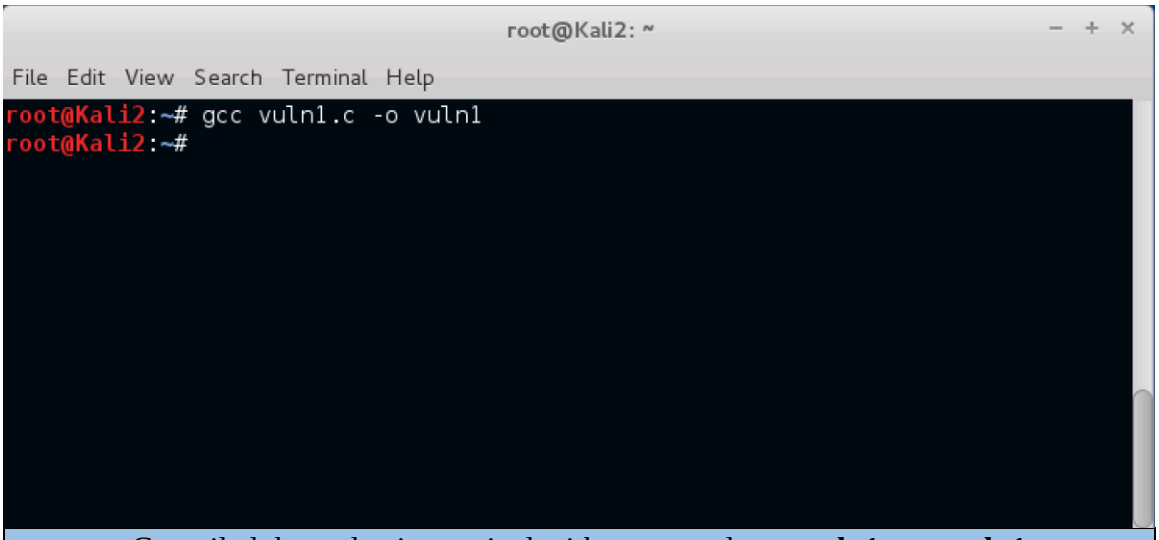
2. Save as



Saved the script file as **vuln1.c** within the leafpad application **root** home directory. Closed the Leafpad application after the file save was complete.

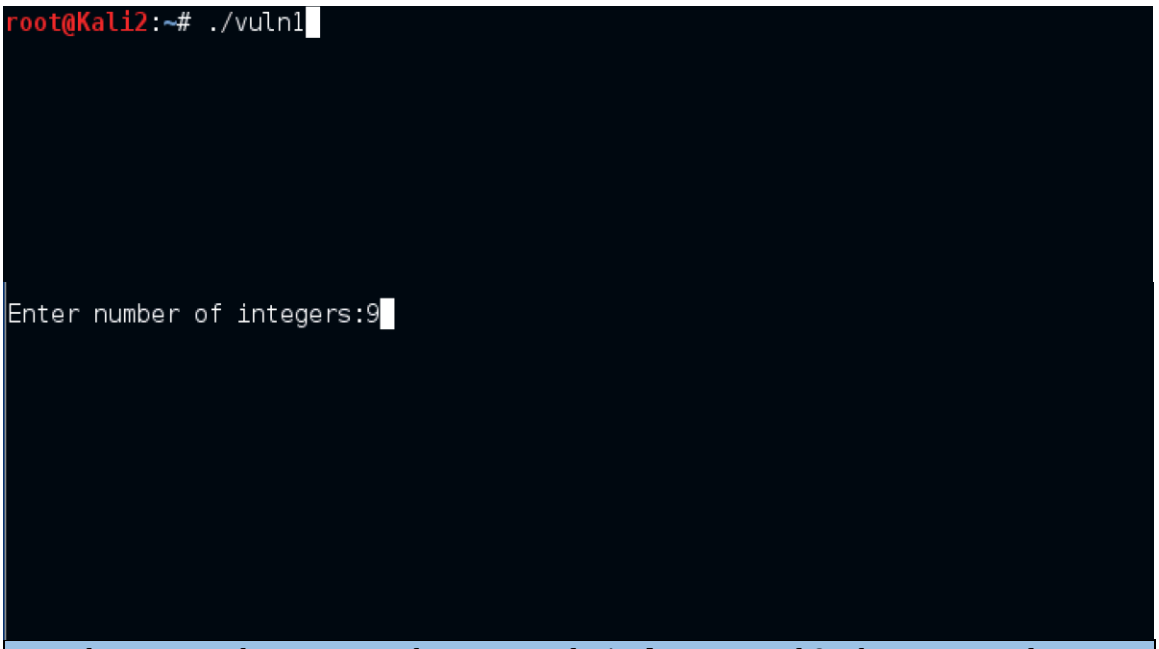
2. Run Code to Demonstrate Buffer Overflow

1. Terminal



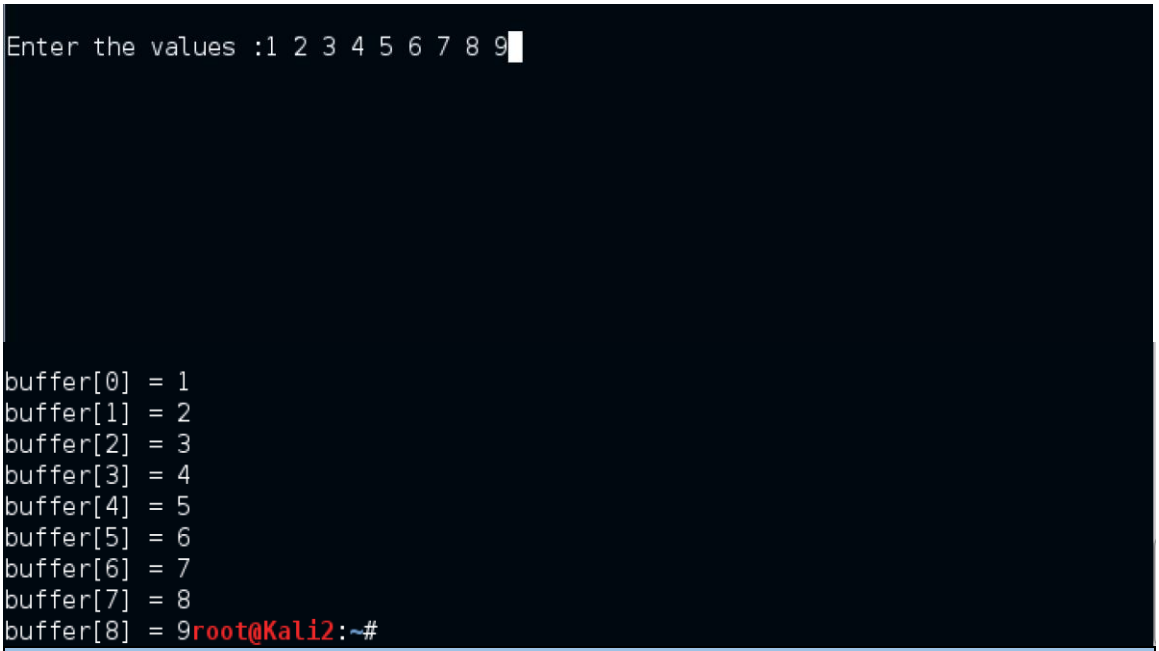
Compiled the code via terminal with command: **gcc vuln1.c –o vuln1**

2. Running the program



Ran the program by inputting the command: **./vuln1**. Entered 9 when prompted to inputt the number of integers then pressed **Enter** on keyboard to execute it.

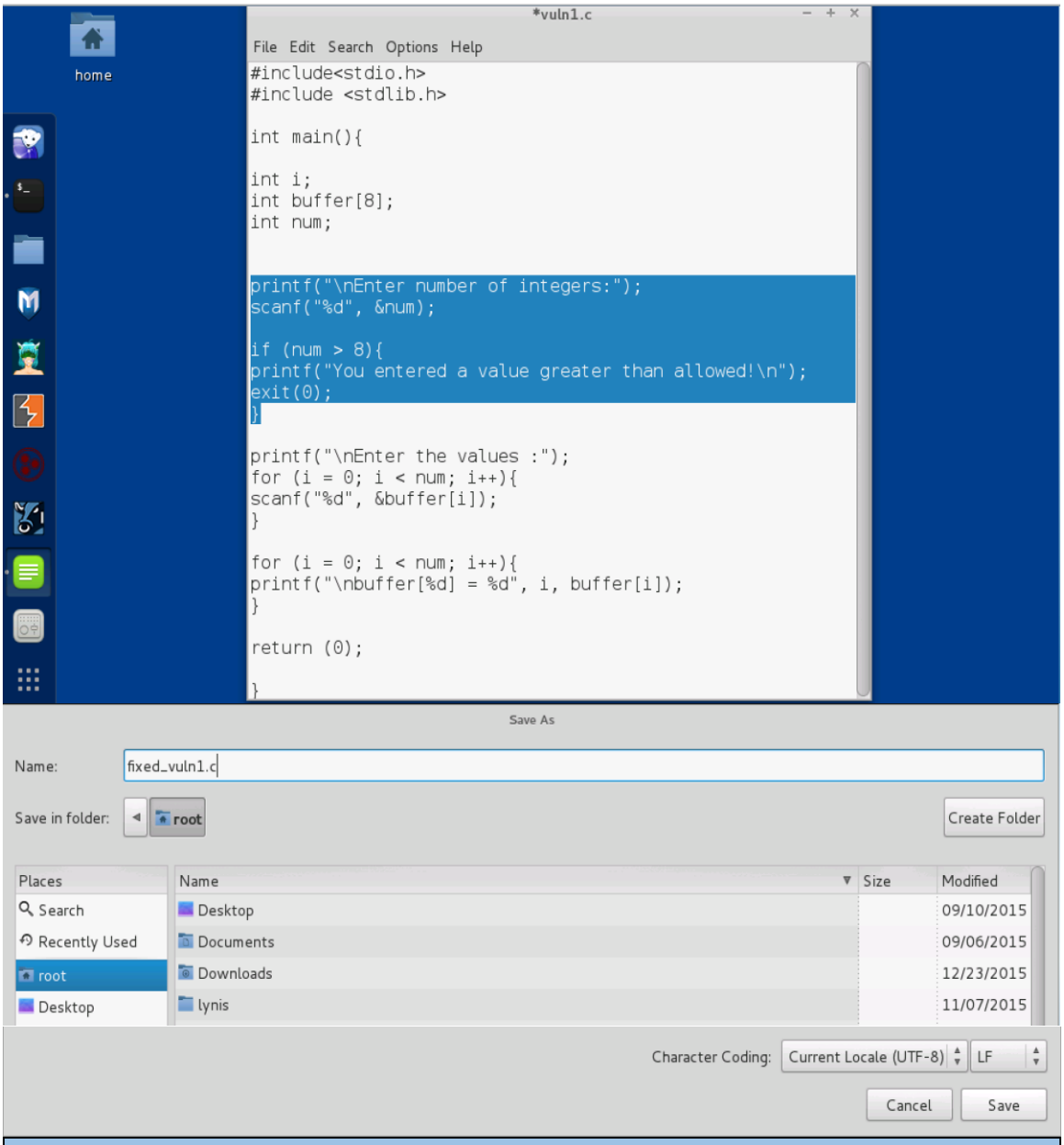
3. Enter the values



Inputted values **1 2 3 4 5 6 7 8 9** when prompted to enter the values. Noticed that a buffer overrun was caused since 9 elements were chosen as opposed to the acceptable 8 elements.

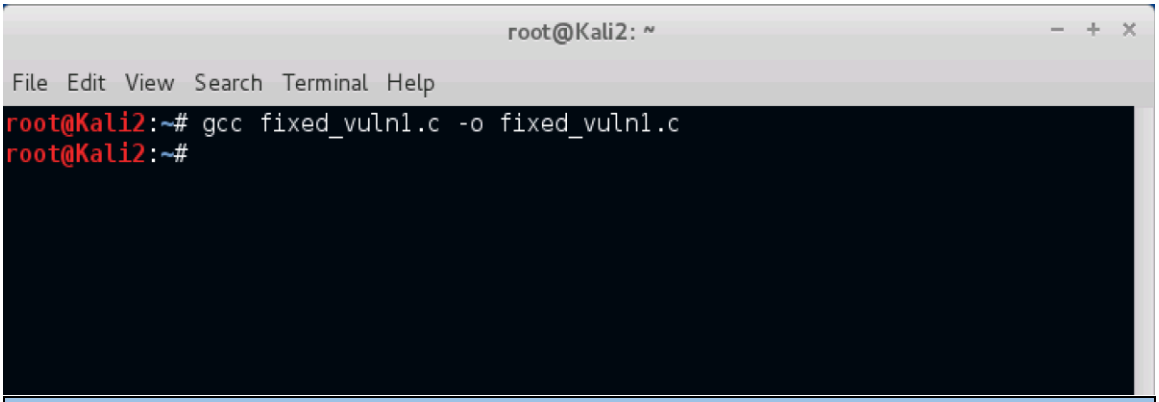
3. Analyzing and Modifying Overflow Code

1. Leafpad application



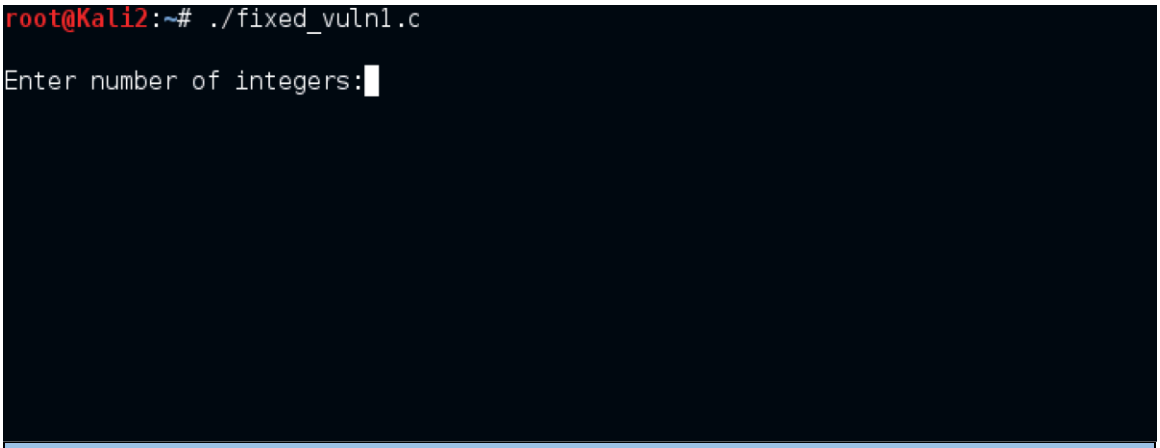
Reopened the **vuln1.c** file to edit the code to prevent an overflow and after the edit, saved the file as fixed_vunl1.c.

2. Terminal



Inputted command: **gcc fixed_vuln1.c –o fixed_vuln1.c** to compile the code for the new **fixed_vuln1.c** program.

3. New code

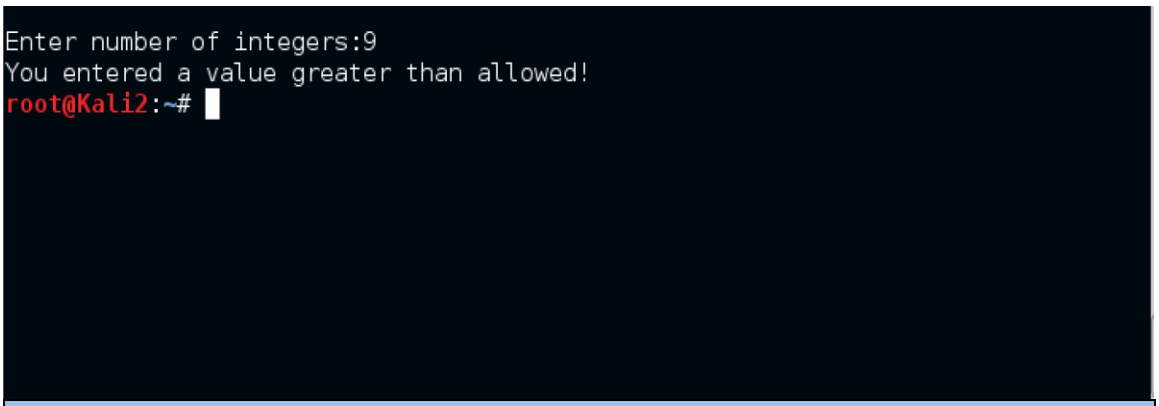


Inputted command: **./fixed_vuln1.c** to run the new code.

4. Number of integers

Entered **9** when prompted to enter the number of integers.

5. Value not allowed



The output now informs that the value entered, is greater than **8**, and the program closes.