



Introduction to Cybersecurity
CS/IS 193

LAB15 REPORT

5/29/2022

DAVID ARCHER

Table of Contents

1. Introduction	3
2. Lab Results	3

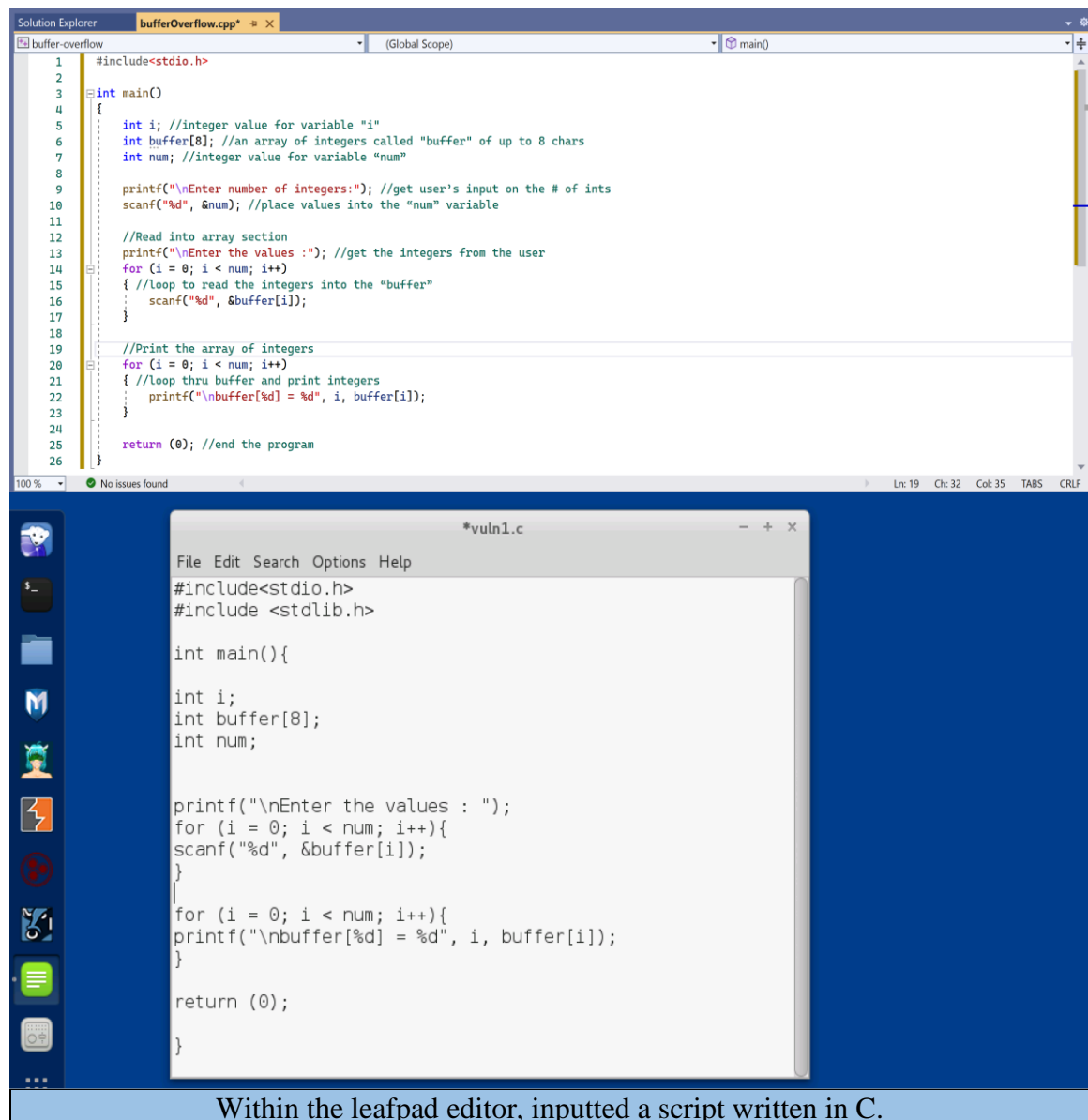
1. Introduction

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



The screenshot displays a Kali Linux virtual machine environment. In the foreground, a terminal window titled '*vuln1.c' shows a C program with the following code:

```
File Edit Search Options Help
#include<stdio.h>
#include <stdlib.h>

int main(){

    int i;
    int buffer[8];
    int num;

    printf("\nEnter the values : ");
    for (i = 0; i < num; i++){
        scanf("%d", &buffer[i]);
    }

    for (i = 0; i < num; i++){
        printf("\nbuffer[%d] = %d", i, buffer[i]);
    }

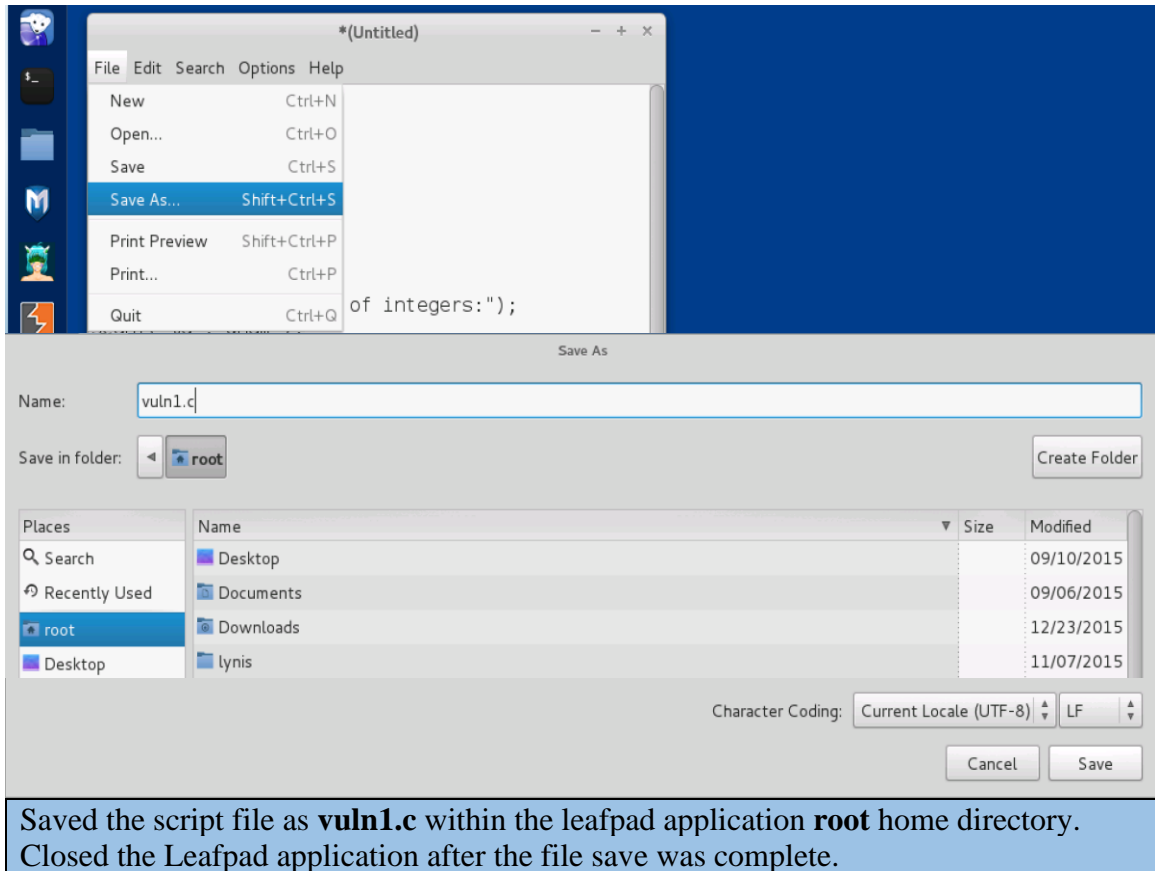
    return (0);
}
```

In the background, a Visual Studio window titled 'bufferOverflow.cpp' shows a C++ program with the following code:

```
Solution Explorer  bufferOverflow.cpp  (Global Scope)  main()
1  #include<stdio.h>
2
3  int main()
4  {
5      int i; //integer value for variable "i"
6      int buffer[8]; //an array of integers called "buffer" of up to 8 chars
7      int num; //integer value for variable "num"
8
9      printf("\nEnter number of integers:"); //get user's input on the # of ints
10     scanf("%d", &num); //place values into the "num" variable
11
12     //Read into array section
13     printf("\nEnter the values :"); //get the integers from the user
14     for (i = 0; i < num; i++)
15     { //Loop to read the integers into the "buffer"
16         scanf("%d", &buffer[i]);
17     }
18
19     //Print the array of integers
20     for (i = 0; i < num; i++)
21     { //Loop thru buffer and print integers
22         printf("\nbuffer[%d] = %d", i, buffer[i]);
23     }
24
25     return (0); //end the program
26 }
```

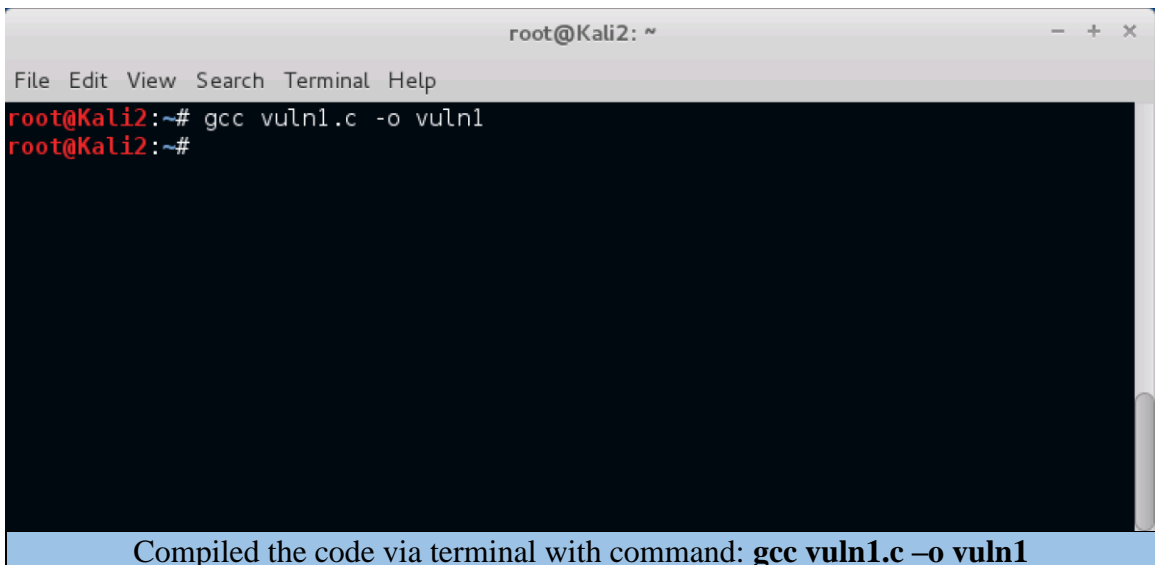
At the bottom of the image, a blue banner contains the text: "Within the leafpad editor, inputted a script written in C."

2. Save as



2. Run Code to Demonstrate Buffer Overflow

1. Terminal



2. Running the program

```
root@Kali2:~# ./vuln1
```

```
Enter number of integers:9
```

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

3. Enter the values

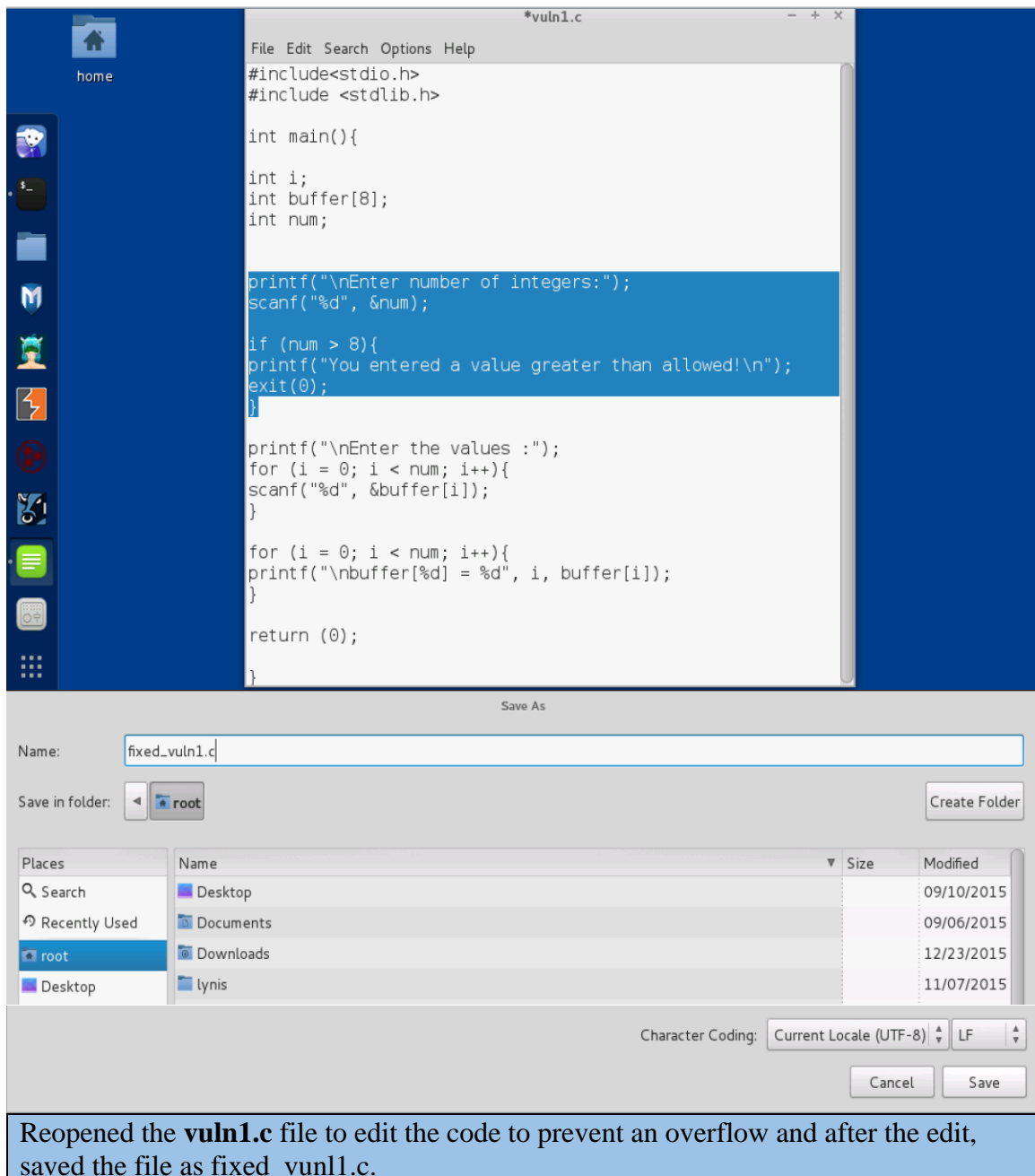
```
Enter the values :1 2 3 4 5 6 7 8 9
```

```
buffer[0] = 1
buffer[1] = 2
buffer[2] = 3
buffer[3] = 4
buffer[4] = 5
buffer[5] = 6
buffer[6] = 7
buffer[7] = 8
buffer[8] = 9root@Kali2:~#
```


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



2. Terminal

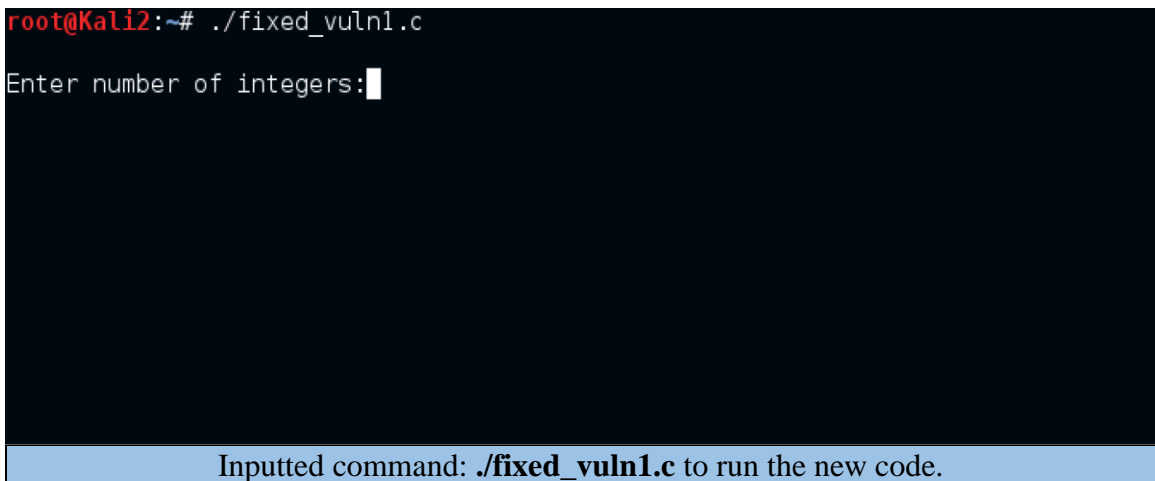


A terminal window titled "root@Kali2: ~" with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command `gcc fixed_vuln1.c -o fixed_vuln1.c` being executed. Below the terminal, a blue box contains the text: "Inputted command: `gcc fixed_vuln1.c -o fixed_vuln1.c` to compile the code for the new `fixed_vuln1.c` program."

```
root@Kali2:~# gcc fixed_vuln1.c -o fixed_vuln1.c
root@Kali2:~#
```

Inputted command: `gcc fixed_vuln1.c -o fixed_vuln1.c` to compile the code for the new `fixed_vuln1.c` program.

3. New code

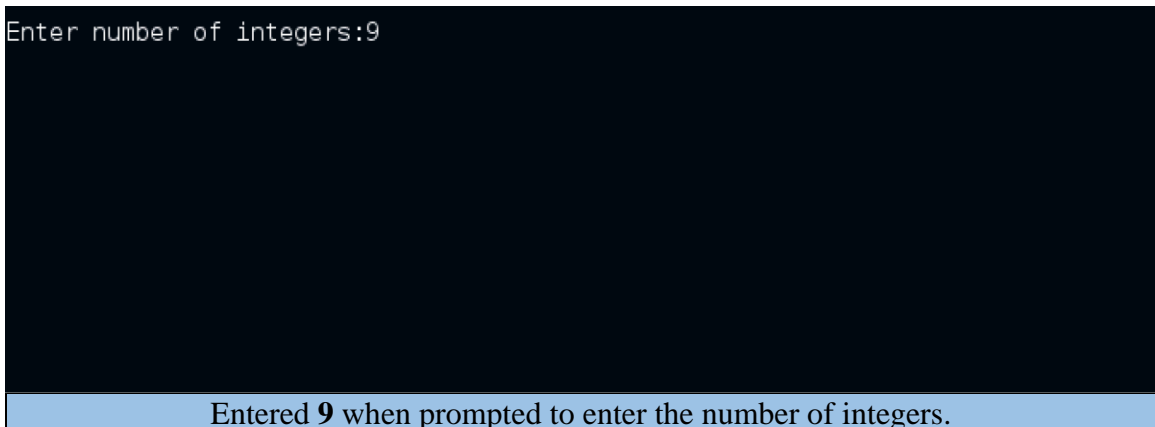


A terminal window showing the command `./fixed_vuln1.c` being executed. The prompt "Enter number of integers:" is displayed with a cursor. Below the terminal, a blue box contains the text: "Inputted command: `./fixed_vuln1.c` to run the new code."

```
root@Kali2:~# ./fixed_vuln1.c
Enter number of integers:█
```

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

4. Number of integers



A terminal window showing the prompt "Enter number of integers:" followed by the input "9". Below the terminal, a blue box contains the text: "Entered **9** when prompted to enter the number of integers."

```
Enter number of integers:9
```

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

5. Value not allowed

```
Enter number of integers:9  
You entered a value greater than allowed!  
root@kali2:~# █
```

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