Central Washington University

Introduction to Computer Security

Spring 2019

Project 3 Report

Author:
Hermann Yepdjio

Instructor:
Dr. Razvan Andonie

May 21, 2019

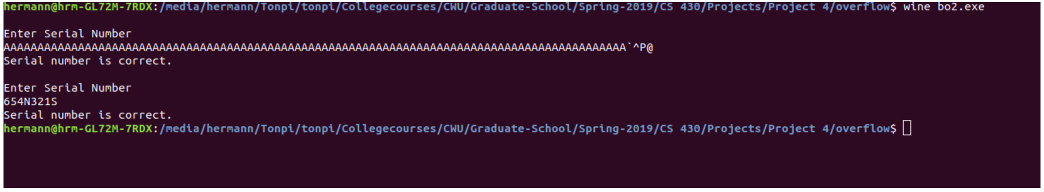
Contents

1 Results

1.1 Problem 1

1.2 Part1

Exploit the buffer overflow so that you bypass its serial number check. Submit a screen capture to verify your success.



```
hermann@hrm-GL72M-7RDX:/media/hermann/Tonpi/tonpi/Collegecourses/CWU/Graduate-School/Spring-2019/CS 430/Projects/Project 4/overflow$ wine bo2.exe

Enter Serial Number
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA`^P@
Serial number is correct.

Enter Serial Number
654N321S
Serial number is correct.
hermann@hrm-GL72M-7RDX:/media/hermann/Tonpi/tonpi/Collegecourses/CWU/Graduate-School/Spring-2019/CS 430/Projects/Project 4/overflow$ 
```

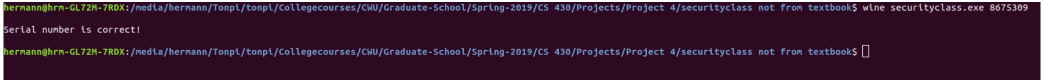
Figure 1: Proof of Buffer Overflow Working for Problem 1

1.2.1 Part2

Using a the disassembler *disasm.exe* found from the internet, we found the serial number to be 654N321S

1.3 Problem 2

Using the program "part2.c" included in the submission package for this assignment, we found the serial number to be 8675309.

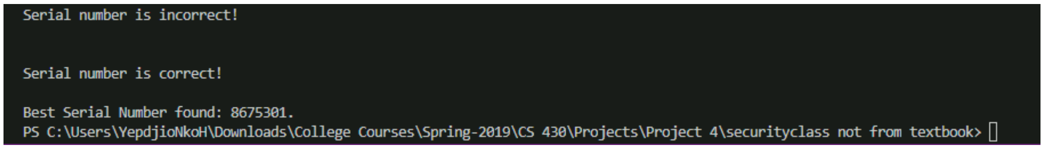


```
hermann@hrm-GL72M-7RDX:/media/hermann/Tonpi/tonpi/Collegecourses/CWU/Graduate-School/Spring-2019/CS 430/Projects/Project 4/securityclass not from textbook$ wine securityclass.exe 8675309

Serial number is correct!

hermann@hrm-GL72M-7RDX:/media/hermann/Tonpi/tonpi/Collegecourses/CWU/Graduate-School/Spring-2019/CS 430/Projects/Project 4/securityclass not from textbook$ 
```

Figure 2: Proof of Serial Number working for Problem 2



```
Serial number is incorrect!


Serial number is correct!

Best Serial Number found: 8675301.
PS C:\Users\YepdjioNkoH\Downloads\College Courses\Spring-2019\CS 430\Projects\Project 4\securityclass not from textbook> 
```

Figure 3: Output of part2.c

2 Observations

As we can see from figure 3 above, the program part2.c finds only the first 6 digits of the serial number and for the last one, we either had to try all digits from 0 to 9 manually or alternatively starting from the last line on the output screen that says if the serial number is correct or not, we counted how many more lines we had to visit (moving upward) until we find a line that says "Serial number is correct!" and subtract that number from 9 to obtain the last digit for the serial number. In our case the last line was the correct line so, we had to visit zero more line in order to find that line. Therefore the last digit of the serial number was 9 - 0 = 9. Another observation is that, part2.c might have to be run multiple times in order to get the correct serial number as the linearization approach relies on the trial time for each potential serial number and that time is not accurate.