# ELEC 377 LAB5 DOCUMENTATION

Aiden Peters, Laeticia Niu

**PASSWORD SAM GAULT USES IN OUR SERVER: Jetta26**

## SELFCOMP.C

Selfcomp.c exploits a buffer overflow vulnerability. It consists of a function doTest() that copies a predefined shellcode stored in the compromise array to a smaller buffer named buffer. The shellcode is a assembly code snippet whose goal is to execute /bin/env by setting up registers and making a system call.

In our shell code, since the address that points towards the environment variable is 0x7ffff7fc600, one of the bytes would be 0x00, which causes a NULL and makes the system think that the code is done. To counteract this, we used 0x01 and then had a decrease counter as the next step.

The different parts of the code include:

main(): This sets an environment variable (MD5) and calls the vulnerable function doTest().

compromise[]: Contains a shellcode represented as hexadecimal bytes.

compromise1[]: A template used to find the correct stack offsets for injecting the shellcode.

doTest(): Copies the content of the compromise array (shellcode) into a smaller buffer array.

The vulnerable point lies in the doTest() function, where the loop copies data from compromise to buffer without any bounds checking. This lack of boundary validation can lead to a buffer overflow vulnerability if the size of compromise exceeds the capacity of buffer.

NOPS – 48

Size - (103) + 48 nops = 152 bytes

Return Address - RSP - 152 = 0x7fffffffe6f0 - 152 = 0x7FFFFFFFE658

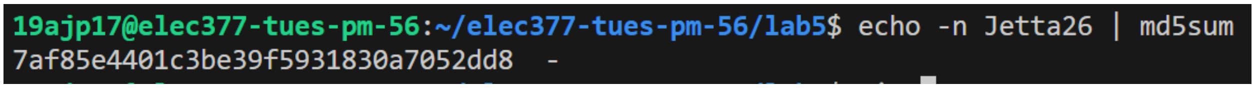
## CLIENT.C

Our client.c code takes in a command line that is the port number associated with ./client. It creates a connection to the TCP client ./quoteserv. The compromise section includes the shell code instructions like the one in selfcomp.c. Using the compromise section, the same buffer overflow exploit used in selfcomp is exploited and the environment variables are pasted to stdout. This includes a MD5 hash password that can be used to determine Sam Gault’s password.

NOPS – 110

Size - (106) + 110 NOPS= 216 bytes

Return Address- sp - 216 = 0x7fffffffe5c8 - 216 = 0x7FFFFFFFE4F0



```
19ajp17@elec377-tues-pm-56:~/elec377-tues-pm-56/lab5$ echo -n Jetta26 | md5sum
7af85e4401c3be39f5931830a7052dd8  -
```

## Seed Words and Numbers

- Sam
- Gault
- Modesto
- Jetta
- Focus
- Sharon
- Grace
- MmmBop
- Tacos
- Purple
- Spot
- Pretzels
- Arizona
- Ruby
- JackAstors
- Winter
- Cashier
- 1997
- 97
- 26

Where applicable, words were tried with and without capitalization.