Buffer Overflow Q&A Workout Analytics

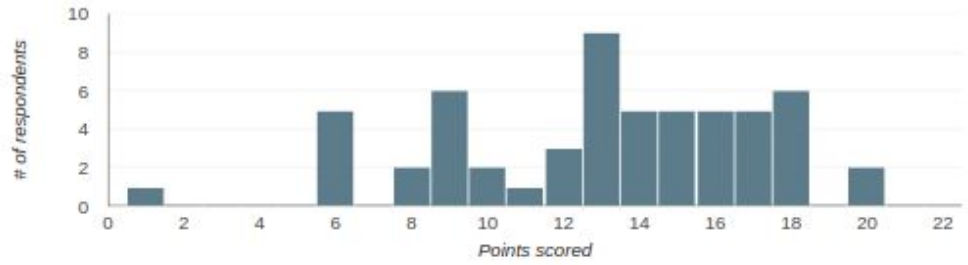
February 14, 2020, CS201P Winter 2020
By Aftab Hussain

Summary (57 Responses)

Insights

Average	Median	Range
13.04 / 22 points	13 / 22 points	1 - 20 points

Total points distribution



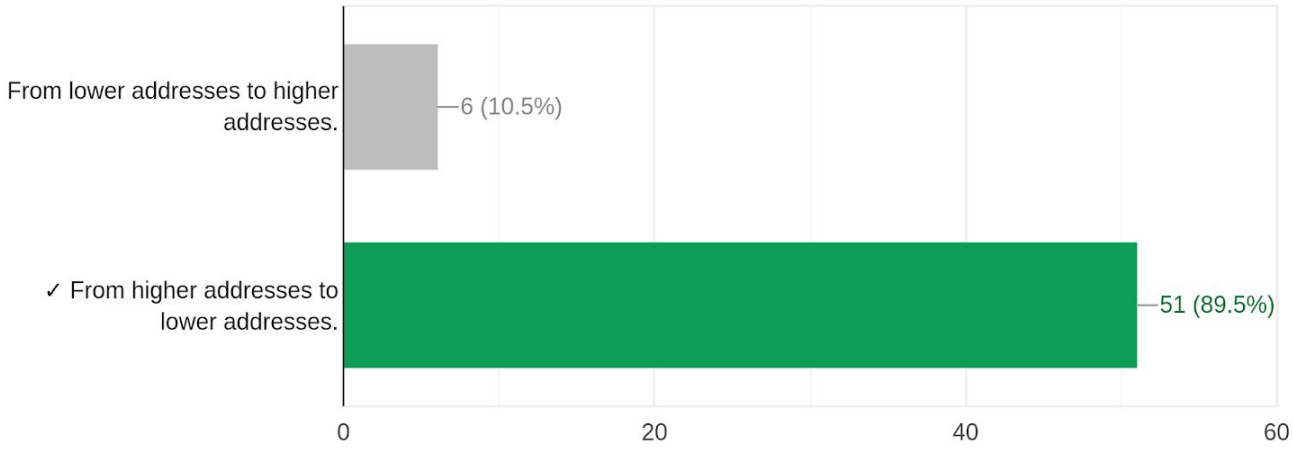
Frequently missed questions

Question	Correct responses
A buffer overflow attack aiming to execute malicious code involves writing over one or more of the following regions of the stack frame from where the attack is initiated. Choose the correct region(s):	21 / 57
During a buffer overflow attack using strcpy(), we provide an address in hex to which we want the execution to jump to. By only seeing them and not knowing what they contain, which of the following addresses could we tell would not work in the attack?	20 / 57
Identify all lines that push "name[0]", the first argument of execve(), into the stack (refer to the corresponding C code above). (Select the relevant line number(s) in the opcode listing above).	7 / 57
Identify all line(s) that push "name", the 2nd argument of execve(), into the stack (Hint: "name" is the address of the name array). (Select the relevant line number(s) in the opcode listing above).	11 / 57
Identify all line(s) that handle the 3rd argument of execve(), NULL, into the stack. (Select the relevant line number(s) in the opcode listing above).	26 / 57

Response Analysis

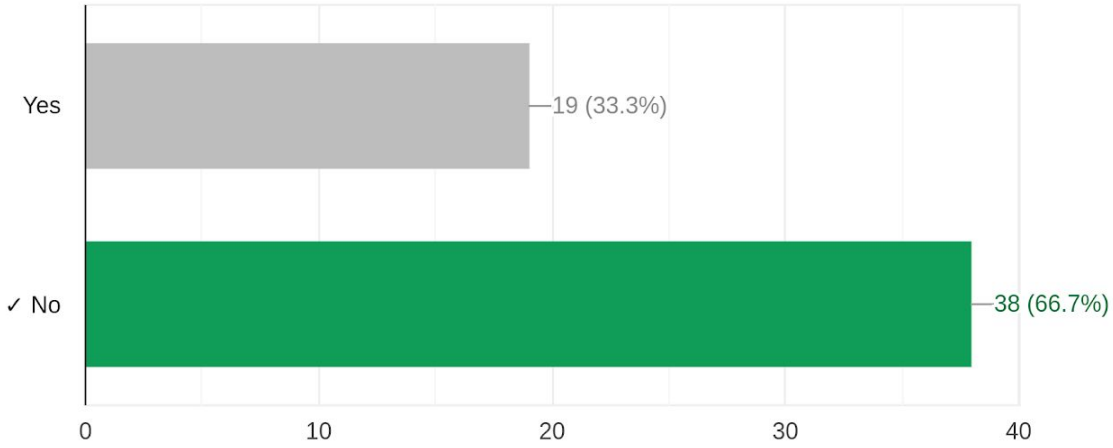
The stack is populated with functions as they are invoked. How does the stack grow in the memory?

51 / 57 correct responses



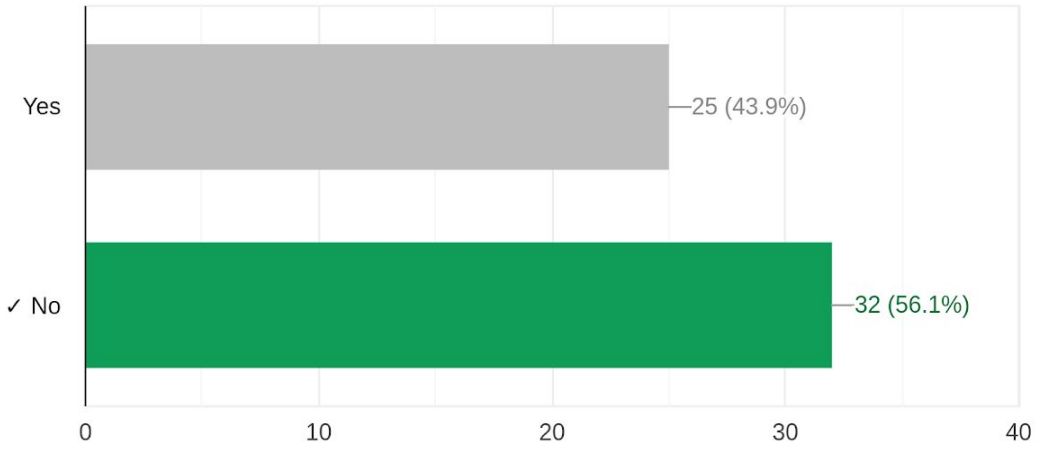
$ebp points to the location of the instruction that follows the call instruction to the current function in the stack frame. Is this true?

38 / 57 correct responses



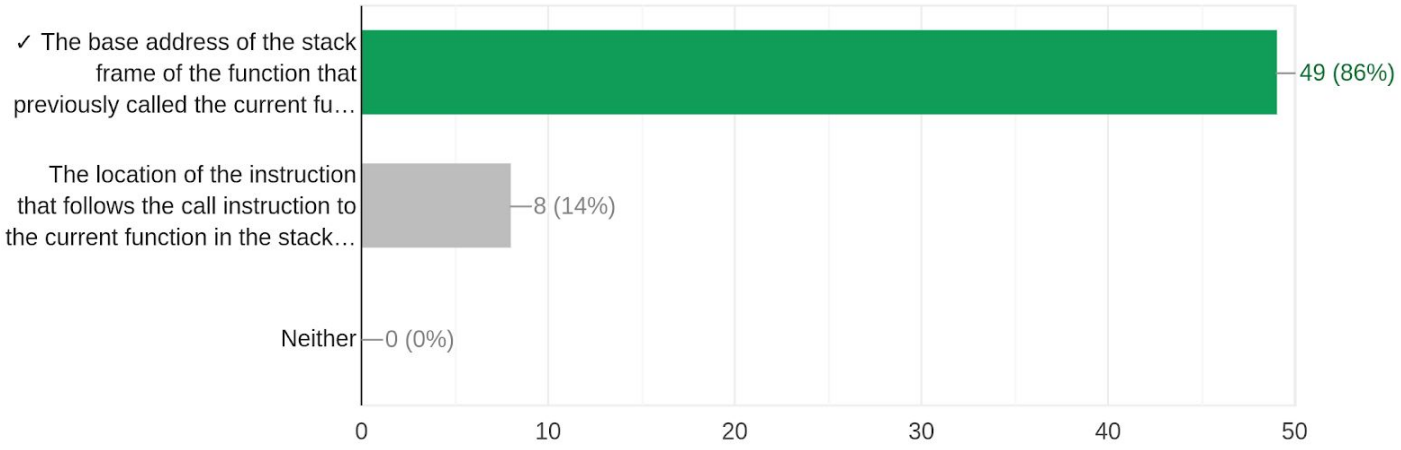
The return address region in the stack frame of a function points to the base address of the stack frame of the function that previously called the current function. Is this true?

32 / 57 correct responses



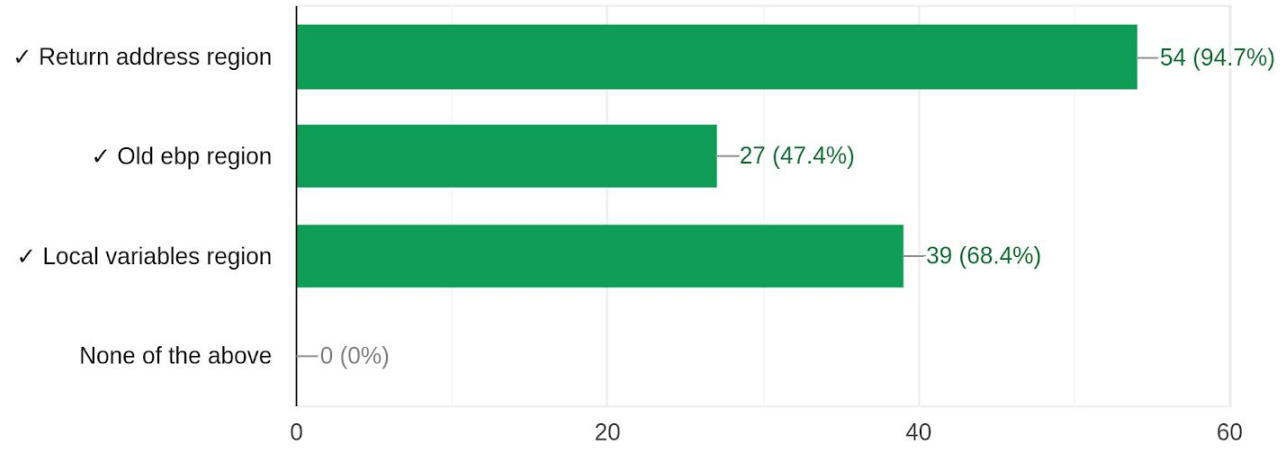
The "oldebp" region of a stack frame points to:

49 / 57 correct responses



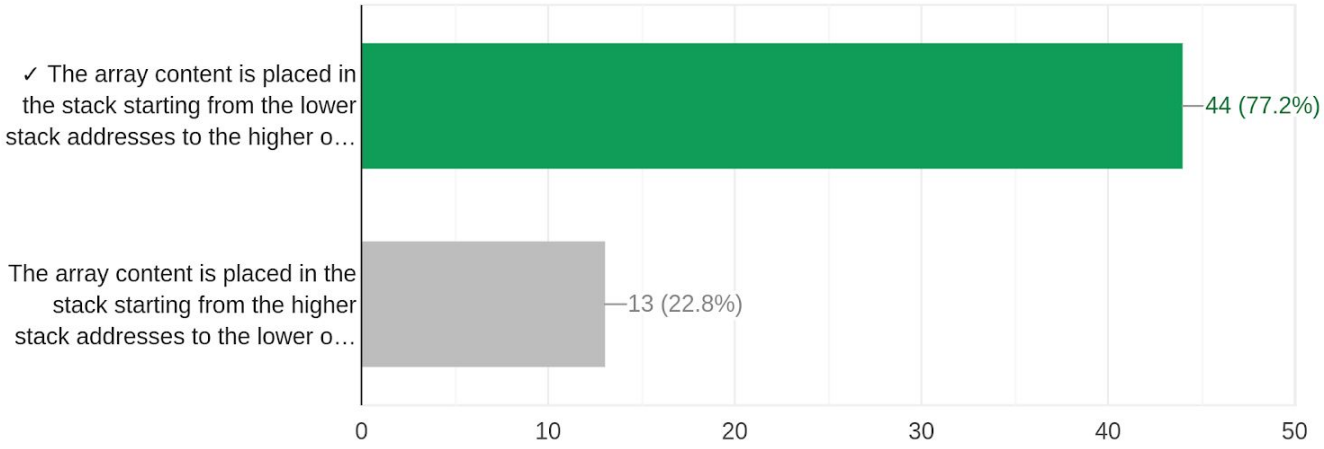
A buffer overflow attack aiming to execute malicious code involves writing over one or more of the following regions of the stack frame from where the attack is initiated. Choose the correct region(s):

21 / 57 correct responses



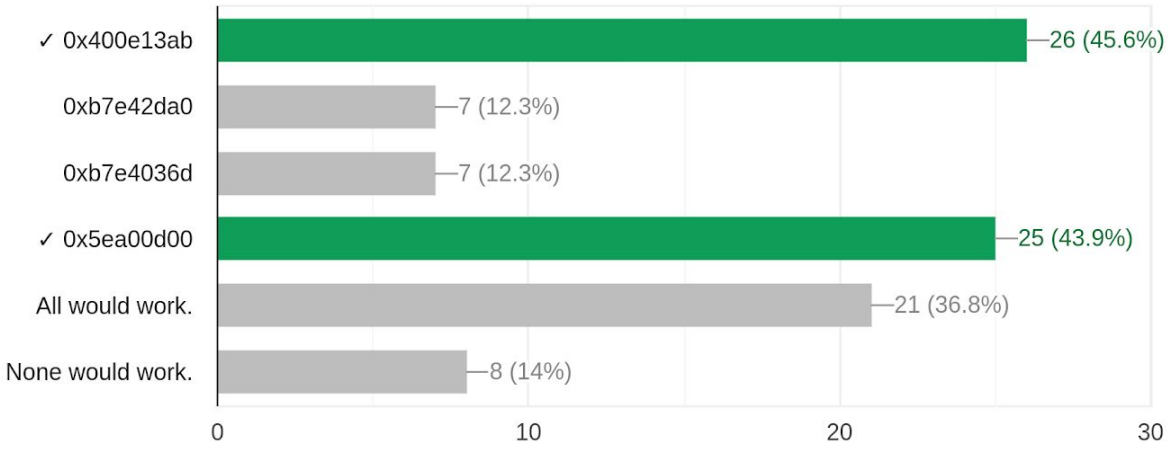
During a buffer overflow attack using strcpy(), you copy a character array. How is the stack populated with the array elements?

44 / 57 correct responses



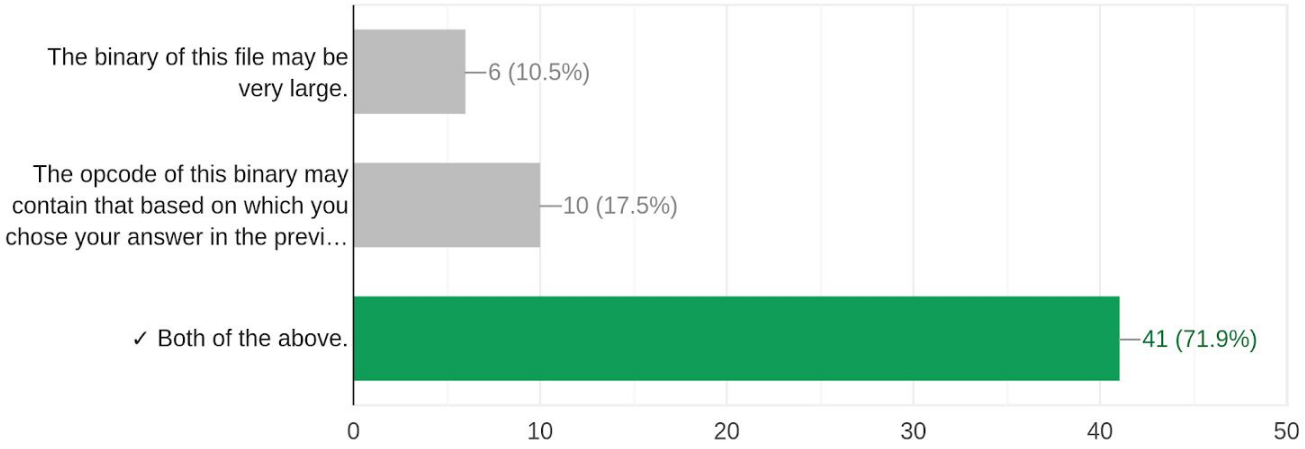
During a buffer overflow attack using strcpy(), we provide an address in hex to which we want the execution to jump to. By only seeing them and not ...resses could we tell would not work in the attack?

20 / 57 correct responses



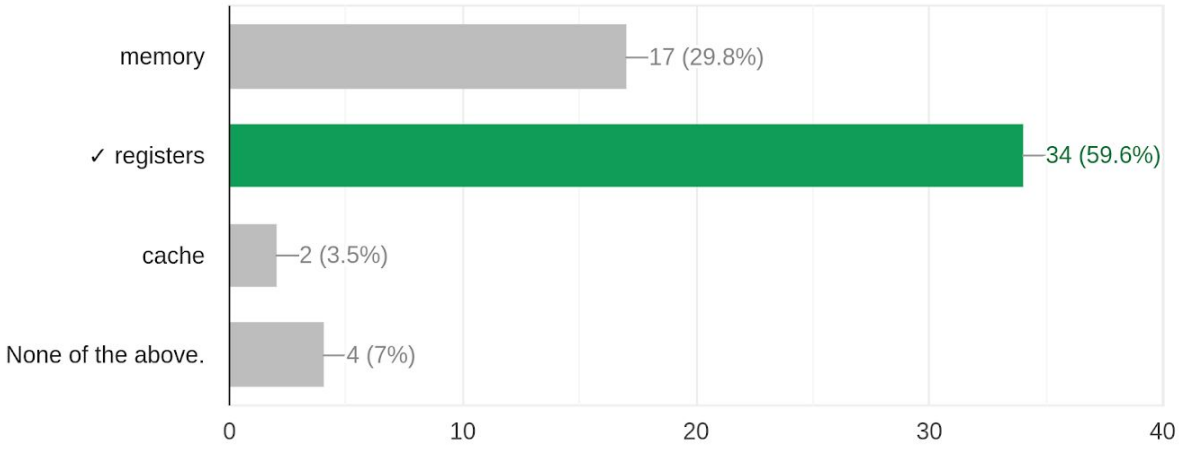
Say we want to execute shell in the target machine using the following C code. A strategy to trigger this in a buffer overflow attack with strcp...he reason(s) why this might not be a good strategy?

41 / 57 correct responses



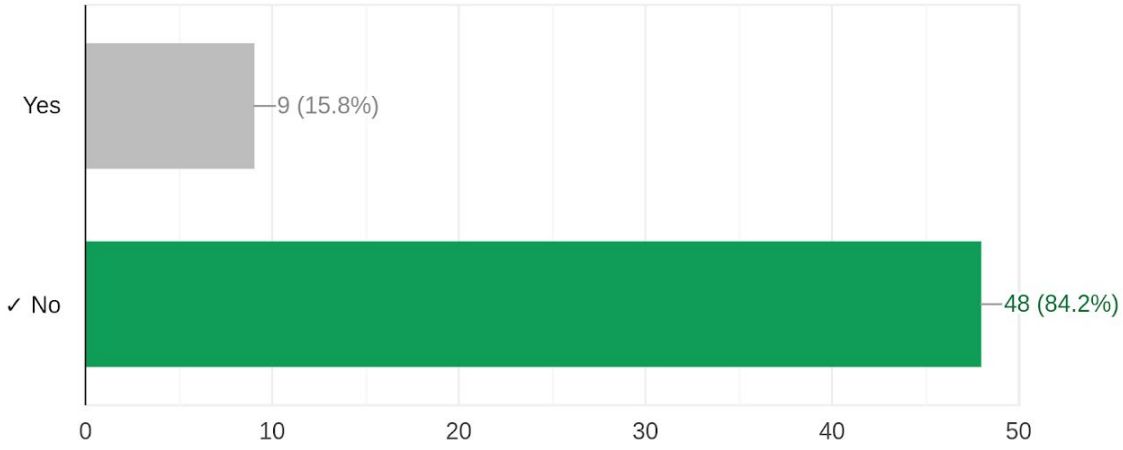
execve() is a system call taking in 3 arguments. Where does it get those arguments from?

34 / 57 correct responses



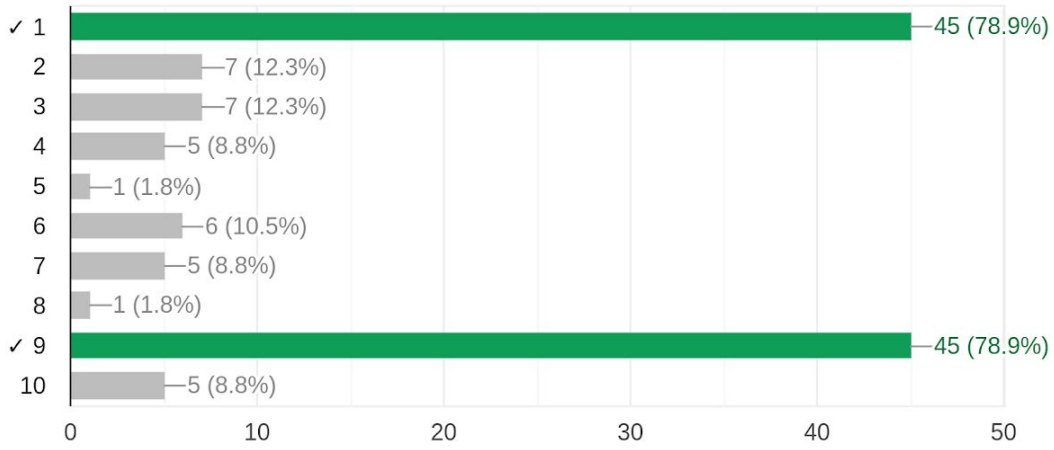
Given that injecting the binary of the C code above in the stack is not a good attack strategy, we decide to inject its machine opcode, as given below...de instruction, Ref. Prof. Du, Computer Security)

48 / 57 correct responses



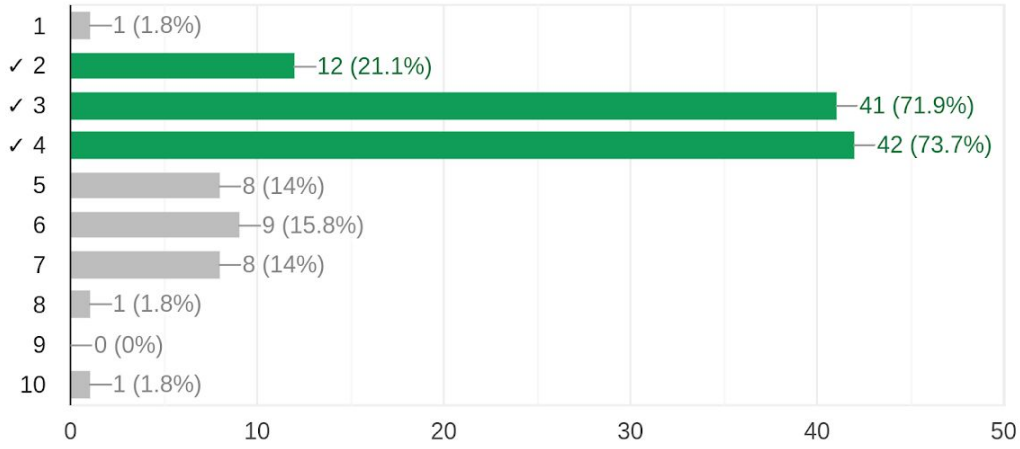
The above opcode has 10 lines of code, let's say the line no. of the first instruction is 1. Identify all line(s) that generate a "0". (Select the relevant line numbers in the opcode listing above).

41 / 57 correct responses



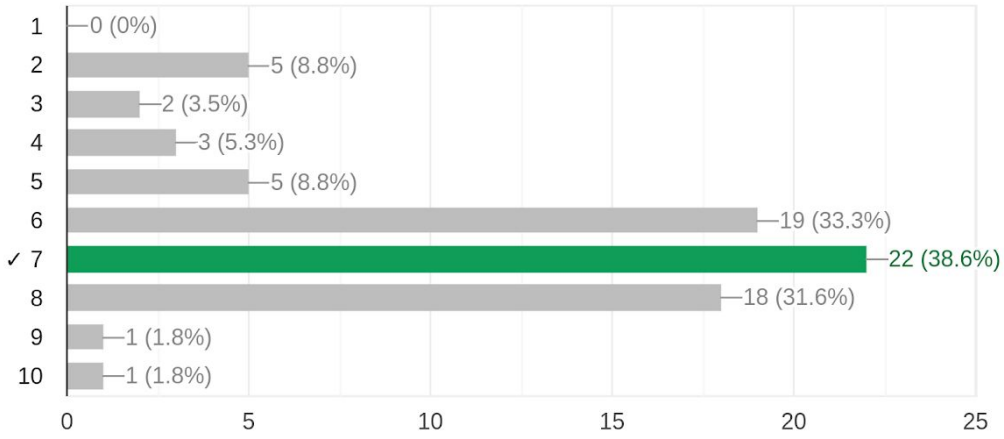
Identify all lines that push "name[0]", the first argument of execve(), into the stack (refer to the corresponding C code above). (Select the relevant line number(s) in the opcode listing above).

7 / 57 correct responses



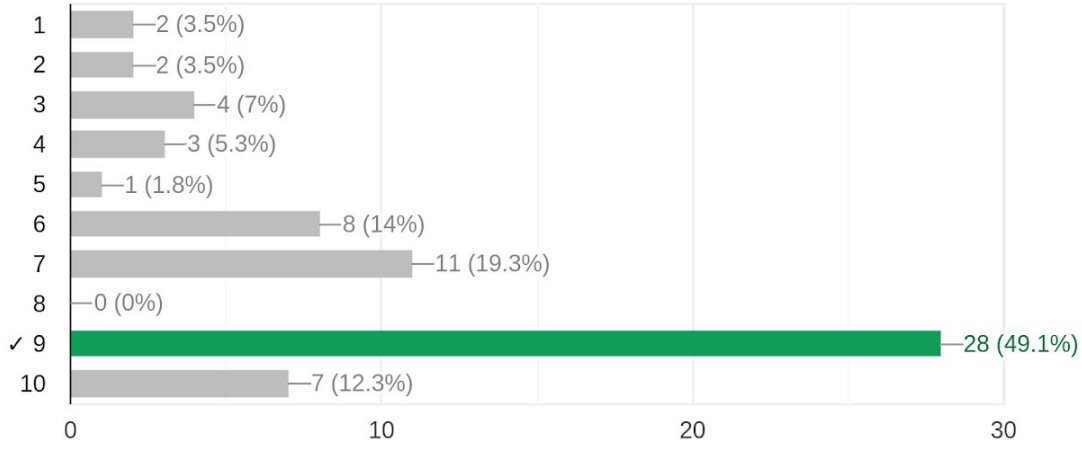
Identify all line(s) that push "name", the 2nd argument of execve(), into the stack (Hint: "name" is the address of the name array). (Select the relevant line number(s) in the opcode listing above).

11 / 57 correct responses



Identify all line(s) that handle the 3rd argument of execve(), NULL, into the stack. (Select the relevant line number(s) in the opcode listing above).

26 / 57 correct responses



Since it is difficult to guess the exact starting address of the exploit code, which we want to execute, which of the following changes do we make to our shell code?

53 / 57 correct responses