VM BOF quiz

12 questions

1 point

1.

Complete this quiz when you have completed project 1. The questions for the quiz were presented in the description of the project, so you should just have to enter your answers here. To make sure your answers match, avoid spurious whitespace.

There is a stack-based overflow in the program. What is the name of the stack-allocated variable that contains the overflowed buffer?

Preview

wis

Please note: Each of the following will be interpreted as a single variable, not as a product of variables: wis. To multiply variables, please use * (e.g. enter x*y to multiply variables x and y).

wis

1 point

2.

Consider the buffer you just identified: Running what line of code will overflow the buffer? (We want the line number, not the code itself.)

62

1 point

3.

There is another vulnerability, *not dependent at all on the first*, involving a *non*-stack-allocated buffer that can be indexed outside its bounds (which, broadly construed, is a kind of buffer overflow). What variable contains this buffer?

Preview

$$ptrs$$

Please note: Each of the following will be interpreted as a single variable, not as a product of variables: ptrs. To multiply variables, please use * (e.g. enter x*y to multiply variables x and y).

ptrs

1 point

4.

Consider the buffer you just identified: Running what line of code overflows the buffer? (We want the number here, not the code itself.)

101

1 point

5.

What is the address of `buf` (the local variable in the `main` function)? Enter the answer in either hexadecimal format (a 0x followed by 8 "digits" 0–9 or a-f, like `0xbfff0014`) or decimal format. Note here that we want the address of `buf`, not its contents.

0xbffff130

1 point

6.

What is the address of `ptrs` (the global variable) ? As with the previous question, use hex or decimal format.

0x804a0d4

1 point

7.

What is the address of `write_secret` (the function) ? Use hex or decimal.

0x8048534

1 point

8.

What is the address of `p` (the local variable in the `main` function) ? Use hex, or decimal format.

0xbffff534

1 point

9.

What input do you provide to the program so that `ptrs[s]` reads (and then tries to execute) the contents of stack variable `p` instead of a function pointer stored in the buffer pointed to by `ptrs`? As a hint, you can determine the answer by performing a little arithmetic on the addresses you have already gathered. If successful, you will end up executing the `pat_on_back` function. Provide the smallest positive integer.

771675416

1 point

10

10.

What do you enter so that `ptrs[s]` reads (and then tries to execute) starting from the 65th byte in `buf`, i.e., the location at `buf[64]`? Enter your answer as an (unsigned) integer.

771675175

---

1 point

11.

What do you replace \color{red}{\verb|\xEE\xEE\xEE\xEE|} with in the following input to the program (which due to the overflow will be filling in the 65th–68th bytes of \color{red}{\verb|buf|}) so that the \color{red}{\verb|ptrs[s]|} operation executes the \color{red}{\verb|write_secret|} function, thus dumping the secret? (Hint: Be sure to take endianness into account.)

\color{red}{\verb|771675175\x00AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\xEE\xEE\xEE\xEE|}

\x34\x85\x04\x08

---

1 point

12.

Suppose you wanted to overflow the `wis` variable to perform a stack smashing attack. You could do this by entering 2 to call `put_wisdom`, and then enter enough bytes to overwrite the return address of that function, replacing it with the address of `write_secret`. How many bytes do you need to enter prior to the address of `write_secret`?

148

I, **Charvik Dipakbhai Patel**, understand that submitting work that isn't my own may result in permanent failure of this course or deactivation of my Coursera account.
Learn more about Coursera's Honor Code

Submit Quiz