Lab 9.1: Buffer Overflow Questions
IN618 Security

April 12, 2016

Instructions

Answer the questions below and submit a hard copy in class on Tuesday, 3 May.

1. When we performed our buffer overflow tests, why did we use "aaaabbbbccccdddd... yyyyzzzz" for our input string? Why not just use a string with one repeated character?

2. When we performed our attack, why did we use the bytes produced by compiling and loading our assembly language code?

3. In our exploit input, what was the significance of the `\x90` characters?

4. We overwrote the return address value as part of our exploit. What was located at the addess we inserted?