

Homework 2

1. Assume format string attacks allow you to read out the stack. What can you do with this information? (Hint: Consider what is stored in the stack.)
2. Assume you can crash a program remotely. Why is this a problem?
3. How can the choice of a programming language help with buffer overflow attacks? (Hint: Why are C-programs prone to such attacks, but not Java programs.)
4. (Optional) How can a system that separates between *users* and *root* be of any help with buffer overflow attacks?