Evgenii Litvinov

Professor Aron Laszka

COSC 3371 / 2021 Spring

April 15, 2021

Homework 3

Problem 1 (2 points): Buffer Overflow:

1. rertyuiopijhgfdss

2. We overflow the old password by using 17 character.

3. “So it begins…”

Problem 2 (2 points): Integer Overflow:

1. 257

2. The char is from 0 - 255 and we add 2 to execute 1 and overflow.

3. “I have come here to chew bubblegum and hack programs, and I’m all out of bubblegum.”

Problem 3 (2 points): Format String Reading:

1. %d%d%d%d%d%d%s

2. Basically, “pop” the stack until you get to the secret with the %d. Also, professor told us “But for this homework, it is fine to just manually figure it out (since we do not have time to learn about gdb).”

3. “What a bug… what a lovely bug!”

Problem 4 (2 point): Filenames and Symbolic Links:

1. rm public.txt -> y -> ln -s /home/secret4.txt public.txt ->. /problem4

2. First argument is what I’m linking to and the second is the file that does the linking. By doing that we get an access to the secret4.txt

3. “… just kidding, this is actually the solution”

Problem 5 (2 extra point for the course): Format String Writing

1. %99d%99d%d%d%n

2. Going upwards in the stack until we reach <<address>> and using the %n placeholder to change your authorization\_level.

3. “Whew, you are finally done with the homework.”