Homework Assignment #9 – Binary Exploitation II

Practical Cyber Security Fundamentals (CTF), Spring 2017
Department of Computer Science, Florida State University

Points: 45
Due: Beginning of the class (5:15pm) on April 3rd, 2017

Submission: You need to submit electronically via Blackboard by uploading a pdf file (named "**hw9-Firstname-Lastname.pdf**") for your answers and programs to the problems; you need to combine all the parts into a single file. Here replace "Firstname" using your first name and replace "Lastname" using your last name in the file name.

All the materials can also be obtained from
https://github.com/n0l3ptr/IntroToCTFs/tree/master/pwn-revisited

Problem 1 (15 points)

Get a flag from warmup (nc fsu-ctf.selfip.net 9983 warmup)

File: http://www.cs.fsu.edu/~liux/courses/ctf/assignments/BinaryExp2/warmup

Problem 2 (15 points)

There are three other files with buffer overflow vulnerabilities, a.out, b.out, and c.out. For each, write how many bytes you need to pad before you can overwrite the return address. Then explain a strategy in detail that could be used to exploit the binary given the protections in place and the available code.

Files: http://www.cs.fsu.edu/~liux/courses/ctf/assignments/BinaryExp2/a.out (nc fsu-ctf.selfip.net 9982 #a.out)
http://www.cs.fsu.edu/~liux/courses/ctf/assignments/BinaryExp2/b.out (nc fsu-ctf.selfip.net 9981 #b.out)
http://www.cs.fsu.edu/~liux/courses/ctf/assignments/BinaryExp2/c.out (nc fsu-ctf.selfip.net 9980 #c.out)

Problem 3 (15 points)

Choose a program from Problem 2 and pop a shell.

.