Assignment 4 – Return Oriented Programming
Due Friday 06/18/21

For this project you are required to understand a vulnerable program and develop an exploit for that program

Setup: The binary for this assignment is available on Sakai.

You will need to get the binary into your virtual machine. Please make certain that you are developing and testing on the VM that is posted on Box (https://nps.box.com/s/3k4ue8uoudkzrod8luaggeliluhwfefj) otherwise your exploit is not likely to work when it gets tested. You are highly encouraged to get an early start on understanding the binary by running the binary on your virtual machine and interacting with it. In addition to deducing the behavior of the binary by interacting with it, you are free to disassemble the binary using any tools at your disposal (such as objdump, IDA, or ghidra) and reading through the disassembly to enhance your understanding of the binary's behavior. You may of course try to deduce the nature of the vulnerabilities by sending unusual inputs, attempting to crash the binary, and observing crashes in a debugger. For this project, randomization will be turned **ON** and the stack will **NOT** be executable.

For testing purposes, the binary will be launched on the target computer with the following command line:

./inetd –p 4567 –e ./final_21

Deliverables: Provide an attack script that exploits the target binary and results in an interactive shell on the target computer that may be interacted with via the target script.