Security Engineering – Winter 2017

Sambuddho Chakravarty

March 9, 2017

Lab Assignment 2 (Total points: 20)

Due date: March 10, 2017. Time: 23:59 Hrs.

Return Oriented Programming

The objective of the assignment is to familiarize you with Return Oriented Programming (ROP). As a part of the assignment you have to write a program that exploits the concept of gadgets that we discussed in the class. Please go through the class lecture slides as well as the additional text posted in the course page also (and also uploaded on backpack). The objective of the assignment is to write a short C program wherein you manually update the stack so that when the program ends the execution jumps to sequence of "POP RET" that populate appropriate registers and thereafter jump to the address of `execve()` function in `libc` library. The sequence of "POP RET" instructions together populate the appropriate registers with address of `'/bin/sh'` string, which is eventually passed to the `execve()` function that leads to the shell being executed. **(20 points)**

For your convenience, a basic C program has be provided as a resource. You may modify the program such that

Bonus Points

Augment the above program so as to print "Hello world!" on `stdout` using sequence of "POP RET" instructions that eventually uses the `write()` system call. **(10 points)**