Networks and Systems Security, Assignment 2
No-penalty due date: March 7, 2022 / 2359 hrs
Total points: 30

Basic buffer-overflow vulnerability exploitation (30 points)

The objective of this assignment is to familiarize you with writing shellcode to exploit programs. You need to write a shell code using Intel X86-64 assembly language using any assembler of your choice (GNU AS, NASM etc.). The shellcode should print ``Hello World!'' on the terminal and thereby exit.

Once you have the shellcode ready you need to devise a way to pass it as an input to a program (victim-exec-stack, shared separately) so that at termination the input code is executed (as it normally happens with shell code execution). The program is written for Linux/X86_64 architecture. The following stack smashing protections have been disabled:

1. Address Space Layout Randomization (ASLR).
2. Stack smashing protection (SSP).
3. Preventing the execution of code from the stack.

Grading Rubric
- Successful compilation of the shellcode using Makefile (5 points).
- Working standalone shellcode that uses system calls (victim) to print ``Hello World'' (10 points).
- Correctly passing the shellcode to the program forcing it to correctly execute it (10 points).
- Description of the shellcode code, commands to test the shellcode and the assumptions that you made (5 points).