Assignment 2

Return-to-libc, String format vuln. And Reverse engineering
CS 4612-01: Secure Software Development, Fall 2023

Due: October 5th

Purpose

The assignment's learning objective is for students to gain first-hand experience on return-to-libc, string format vulnerability, and reverse attacks by running codes to demo and show what they have learned about vulnerabilities from class into action.

Activities:

1) You are given a program with a buffer overflow vulnerability; your task is to develop a **`return-to-libc`** attack to exploit the vulnerability and finally to gain the root privilege. (**exploit_libc.py, stack.c, envaddr.c files are given**)

2) You will need to use the (format string) printf statement to:
   (a) crash the program (**file vul.c. see instruction in slides(p16-p21) or textbook**)
   (b) read from an arbitrary memory place. **Use instruction from** (2a)
   (c) modify the values of in an arbitrary memory place. **Use instruction from** (2a)

3) You are given a program with uncalled functions, you will need to point your next instruction register to the function's address to run it**.**
Use instructions from reverse engineering. See file eipExercise.c, run cannotReach and untouchableFunction.

Use Ubuntu 16.04, it is 32bit.

Resources:
Install virtual box
https://www.virtualmetric.com/blog/how-to-enable-hardware-virtualization
https://www.virtualbox.org/wiki/Download_Old_Builds_6_0
Setup ubuntu https://releases.ubuntu.com/16.04/

Question 1: return-to-libc attack:
Question 2: String format vulnerability:
Question 3: Reverse engineering:

Deliverables: Video demo of your implementation with your face at the corner of your screen. You will talk and explain over the video as the program runs; you will tell how you set the environment, run each command, and tell what each command does, and their outputs shown on screen.