Assignment 1: Buffer Overflow (100 points)

Secure Systems Engineering (CS6570)

Deadline: 6/2/25

Problem:

1) You are provided with a binary named *"lab1"* that contains buffer overflow vulnerability, similar to the one demonstrated in the tutorial class but protected by additional *self implemented canary.*

   Can you bypass the current implementation of the binary to execute buffer overflow and execute the **exploit function** bypassing the canary countermeasure implemented? (5 points)

2) You are given a binary named *"main"* that performs authentication for the user. It asks you for the username and reads the password from a file named **private_key.** Your job is to generate an exploit that can bypass the authentication check. There are two parts to this problem:
   a) Write an exploit that can bypass the authentication. (30 points)
   b) Write an exploit that can call the **secret_function.** (40 points)

   To run the binary you need to create a file with the name **private_key** in the same directory with the password.

Submission Guidelines:

- The teams need to download the binaries corresponding to their teams from the folders provided here and create a payload that exploits the two binaries.
- The teams need to submit the two payloads as payload_1 for part 1 and a script, exploit.sh that exploits the binary for part 2.

- Your solutions will be tested on the VM provided to you.
- Other than the payloads the teams need to submit a **report** explaining their approach for generating the payloads. Please mention all the resources used to solve the assignment in your report. (25 points)
- Include Screenshots of the terminal in the report showing a successful exploitation.
- The payloads would be evaluated using a scripts that runs as follows:
    - a) ./lab_1a $(cat payload_1)
    - b) ./exploit.sh (exploit can be written in any language of your choice, provide the instructions in report on how to run it)

Any submission that fails to execute the attack for the above automated scripts on the VM provided would not be considered as the correct solution. There would be no partial markings for these submissions and the teams would then be eligible only for the marks corresponding to the report.

Bonus:

There is a bonus of making a **clean exit** for **both the parts of the assignment**. Any team who does these can use the acquired bonus in the CTF conducted at the end of the course.

Useful tools:

- Ghidra
- GDB