Assignment 2: Ret2libc (100 points)

Secure Systems Engineering (CS6570)

Deadline: 27/2/25

Problem:

We are welcoming new students to Hogwarts at "**nc 10.21.235.155 9999** " and along with it there is a possibility to ensure that Griffindor wins the House cup. To give you a better idea about the hosted binary that's welcoming the students we also provide a similar copy of it to you here. Your goal is to exploit the vulnerability present in the provided binary to ensure that Gryffindor wins the House cup.

(75 points)

Submission Guidelines:

- Teams should submit the **script** to exploit the hosted binary to get all the points.
- 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)

Marking Scheme for the Report

- Explanation of the vulnerability - 2
- Explanation for the working of your payload - 12
- Difficulties encountered and how u resolved them - 5
- Acknowledgement for the folks u discussed the ideas with/internet references used - 2
- Defence mechanisms for the vulnerabilities exploited - 4

Useful tools:

- Ghidra
- pwn_tools