Pwn Challenge (15 points)

We care a lot about the security of our remote grep service: we have compiled it with all the available protections, and on top of that we have added our own innovative stack-canary scheme. You can access the service over the internet, with nc.
The source code and the binary is available here: https://lettieri.iet.unipi.it/hacking/2022-02-24.tar.gz

You can request two hints on the solution:

- Hint #1: Analysis of the bug. Cost: -3 points.
- Hint #2: Attack plan. Cost: -2 points.

Web Challenge (15 points)

FromMeToYou is a website that measures the "distance" from itself to another host in the Internet whose IP address/hostname is provided by the user. The distance is expressed in terms of "hops", which seem to be something related to "routing" or similar. To do that, FromMeToYou uses a highly esoteric thing called "traceroute" or something like that. The candidate must steal the flag that is stored in a "flag" file in the document root of the server.

You can request two hints on the solution:

- Hint #1. Analysis of the vulnerability. Cost: -3.5 points.
- Hint #2. Exploit strategy. Cost: -1.5 points.