Extra Credit: x86 reverse engineering

Due date: see course website
You must do all work individually, and you must submit your work electronically via Sakai.

Here’s a fun exercise for those of you that want to play with reverse engineering and the x86 assembly language. We have prepared two Linux executable files for each student in the course: spy1-<NETID> and spy2-<NETID>, where <NETID> is your Duke NetID. These can be found in spy-<NETID>.tgz.

Each program takes a single argument: a password. If the correct password is provided, the program reveals a short text secret. See the example run below, where the passwords are known.

Here we see that the password for spy1 in this case is “hand7”, which provides the secret “healthy table”. The password for spy2 here was “cup0” which provides secret “past carriage”. All passwords are a simple English word and a single digit, and all secrets are an adjective/noun combination. The two programs work the same way, except the spy2 program is a bit fancier in how it obscures its data internally.

Here is the challenge: you will not be given either password. Instead, you must use any means of analysis you wish (short of getting help from someone else) to obtain the passwords and/or secrets.

Rubric:

- 4 points for the secret in the spy1 program associated with your NetID.
- 4 points for the password to the spy1 program associated with your NetID.
- 4 points for the secret in the spy2 program associated with your NetID.
- 4 points for the password to the spy2 program associated with your NetID.
- 4 points if you get all of the above.

To apply for this extra credit, submit a PDF with your answers and an explanation of how you obtained them, including screenshots.

Points awarded will be added to your homework score, which itself is 55% of the grade. If you do the math, a perfect submission is worth about a 1.6% bump to your course grade.