

Extra Credit: x86 reverse engineering

Due date: see course website

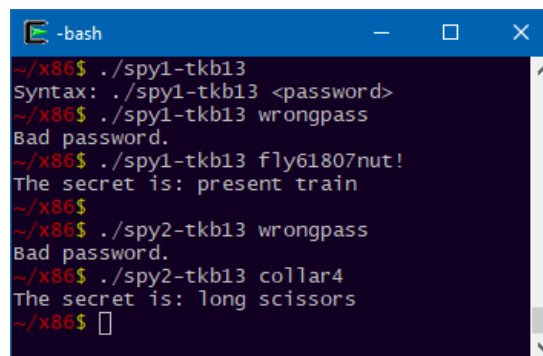
You must do all work **individually**, and you must submit your work electronically via GradeScope.

Here's a fun exercise for those of you that want to play with reverse engineering and the x86 assembly language.

Spy programs

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.



```
-bash
~/x86$ ./spy1-tkb13
Syntax: ./spy1-tkb13 <password>
~/x86$ ./spy1-tkb13 wrongpass
Bad password.
~/x86$ ./spy1-tkb13 fly61807nut!
The secret is: present train
~/x86$
~/x86$ ./spy2-tkb13 wrongpass
Bad password.
~/x86$ ./spy2-tkb13 collar4
The secret is: long scissors
~/x86$
```

Here we see that the password for `spy1` in this case is “fly61807nut!”, which provides the secret “present train”. The password for `spy2` here was “collar4” which provides secret “long scissors”. Passwords for `spy2` are a simple English word and a single digit, passwords for `spy1` are more complex, 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, and `spy1` delays for a second before providing output.

Here is the challenge: you will not be given either password. Instead, you must use any means of analysis you wish (short of getting unauthorized help from someone) 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.

Hardmode challenge

In addition to the above, there's also another challenge. A binary called `hardmode` is provided on the course site (separate from the spy files). This executable contains a function that will, if some conditions are met, render a cool graphic of a well-known video game character to the terminal, but this function is never called at all.

Showing a screenshot of the graphic and a guide to how you achieved it will award you 5 additional points.

Submitting your work

To apply for this extra credit, submit a PDF with your **answers** and an **explanation of how you obtained them, including screenshots**. **Answers that do not show work will not receive credit!**

Submit your PDF to GradeScope's "Extra credit" assignment.

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 2% bump to your course grade.