

Reverse Engineering Project

Massih Majidi

Your task is to crack the executable and retrieve the quote by Mahatma Gandhi. You can accomplish this using the tools and methods presented in the class plus a little bit of creativity.

- Each student must crack his/her own file marked with their student number. Download the executable from the course website or the Telegram channel.
- You must create a cracked version of your executable using patching techniques. The cracked version must allow the user to see the quote without the need to know the correct password.
- Executables differ for each student, and so does the password and the quote.
- Create a patch file using the `bsdiff` command. A patch file contains information about the difference between the two versions of a file. Using a patch file, you can update a file just by updating the parts that need to change. The patch file can be later applied to an old file using the `bspatch` command. You can find out more about patch files, `bsdiff`, and `bspatch` commands here:
 - [https://en.wikipedia.org/wiki/Patch_\(Unix\)](https://en.wikipedia.org/wiki/Patch_(Unix))
 - <http://manpages.ubuntu.com/manpages/bionic/man1/bsdiff.1.htm>
 - <http://manpages.ubuntu.com/manpages/bionic/man1/bspatch.1.htm>

You must also present how you cracked the executable in person to the TAs. You will do this at the time of presenting your final project. They will ask you questions to assess your grip on the homework. Further details about the deadline and how to deliver the project will be posted on the Telegram channel.

Extra Credit!

It is not necessary to find the password in order to crack the file. But you will get extra credit for finding the password as well. Keep in mind that this part will be checked only if you have successfully completed the previous part.

GOOD LUCK!