

Homework 5

Hamid Mohammadi, Amin Parchami

Alice has just got a new homework on Mahatma Gandhi's quotes. The quotes, however, are hidden in password protected applications. She needs your help to crack the files and find the quotes.

Your task is to crack the executable and retrieve the quote by Mahatma Gandhi. You can accomplish this task 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 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 are changed in the recent update. The patch file can be later applied to an old file using the `bspatch` command. You can find out more about patch file, `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.html>
 - <http://manpages.ubuntu.com/manpages/bionic/man1/bspatch.1.html>

Upload only the patch file created using **bsdiff** on courses.kntu.ac.ir by the deadline.

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.