CYB101 Project 3 (🔗 <u>Instructions Page</u>)

👤 Student Name: Harshit Garg

✉️ Student Email: iharshit.garg.cs@gmail.com

Reflection (Required)

🤔 **Reflection Question #1:** If I had to **explain "password security" in 3 emojis,** they would be… (Feel free to put other comments about your experience in this unit here, too!)

🧐🤔😮

🛡️**Reflection Question #2:** What factors make a password hash difficult to crack? Does that match with usual "password requirements" for signing up to websites?

In my opinion, passwords of more than 8 characters containing symbols and numbers are the hardest ones to crack. It is not exactly the same as the password requirements for signing up the websites.

📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

Password Cracking Challenge (Required)

Use the answer boxes below to input your screenshots and example commands for this project. Clarifying notes are optional.

Total Number of Cracked Hashes (Screenshot of output from `john --show CPLeak.txt`)

Notes (Optional):

Sample `john` commands

Please type or copy-and-paste your commands into the boxes below. You do not need to include screenshots of running the commands.

Command #1: a `john` command using **a different wordlist** (not lower.lst)

john --wordlist=rockyou.txt CPLeak.txt

Command #2: a `john` command using **a built-in ruleset**

john --rules:jumbo --wordlist=rockyou.txt CPLeak.txt

Command #3: a `john` command using **a custom mask**

John --mask=?l?l?d?d?d?S --wordlist=rockyou.txt CPLeak.txt