**CYB101 Project 3 (🔗** [**Instructions Page**](https://courses.codepath.org/courses/cyb101/unit/3#!projects)**)**

👤 Student Name: Sila Tamang

✉️ Student Email: stamang3@uco.edu

**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 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? |
| --- |
| A password hash is considered difficult to crack if it satisfies the following factors:   1. Strong cryptographic algorithm: A strong cryptographic algorithm makes it difficult for an attacker to reverse engineer the password from the hash. Hash functions like bcrypt, scrypt, and Argon2 are commonly considered secure for password storage. 2. Length and complexity: Longer and more complex passwords are generally more difficult to crack. Passwords that are at least 12-14 characters long and contain a mix of uppercase and lowercase letters, numbers, and special characters are generally considered more secure. 3. Unique per user: A unique salt for each user's password hash makes it more difficult for attackers to use precomputed tables or rainbow tables to crack passwords en masse. 4. Key stretching: Key stretching is a technique that slows down the password hashing process, making it more time-consuming and resource-intensive for an attacker to crack. Algorithms like bcrypt and scrypt implement key stretching.   These factors do align with some of the usual "password requirements" for signing up to websites. Many websites have requirements for password length and complexity, and some sites use strong password hashing algorithms like bcrypt or Argon2. Additionally, many sites use unique salts for each user's password hash.  However, there are still many sites that do not implement these best practices for password storage, which can leave user passwords vulnerable to cracking. It is important for websites to follow these best practices to protect user passwords and ensure their security. |

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

**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 --format=md5crypt-long --wordlist=/usr/share/wordlists/rockyou.txt --min-length=3 --max-length=8 --mask=?w?d CPLeak.txt** |

#### 

| **Command #2:** a **john** command using **a built-in ruleset** |
| --- |
| **john --wordlist=lower.lst crackChallenge.txt --rules=Jumbo** |

#### 

| **Command #3:** a **john** command using **a custom mask** |
| --- |
| **john --mask=?l?l?l?l?l?d?d?d?d?d --max-length=5 crackChallenge.txt** |

**Submission Checklist**

**👉***Check off each of the features you have completed.* ***You will only be graded on the features you check off.***

**Reflection**

* ~~Reflection Question #1 answered above~~
* ~~Reflection Question #2 answered above~~

**Required Challenge**

* ~~Screenshot of Total Passwords Cracked~~
  + ~~250+ Passwords Cracked~~
* ~~Command #1~~
* ~~Command #2~~
* ~~Command #3~~

**Stretch Challenge**

* 500+ Passwords Cracked
* 750+ Passwords Cracked
* 1000 Passwords Cracked

**Submit your work!**

| Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can edit. (This allows our grading team to input your grade below!)      Step 2: **Copy** the link to this document.    Step 3: **Submit** the link on the portal. |
| --- |

**Grader Comments**

| *Once your project has been assessed, our graders will leave feedback for you in this space. Please do not delete.* **Grading Rubric**  | Reflection Questions | Total Received | Total Possible | | --- | --- | --- | | Reflection Question #1 answered above | 2 | 2 | | Reflection Question #2 answered above | 2 | 2 | | **PART A TOTAL** | 4 | **4** | | Password Cracking Challenge | Total Received Points | Total Possible | | Screenshot of Total Passwords Cracked, showing 250+ Cracks | 7 | 7 | | Command #1 | 3 | 3 | | Command #2 | 3 | 3 | | Command #3 | 3 | 3 | | **PART B TOTAL** | **16** | **16** | | Stretch Challenge | Total Received Points | Total Possible | | 500+ Passwords Cracked | 0 | +1 bonus | | 750+ Passwords Cracked | 0 | +1 bonus | | 1000 Passwords Cracked | 0 | +1 bonus | | **Total Possible Points (Part A + Part B)** | **20** | **20** (+3) | |  |  |  |   **Grader Feedback** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |