Activity 1.1.4 - Hashing + Salts with CyberChef

Observe how adding a salt when hashing a password will protect against a Rainbow Table attack.

First, watch the video Exploring the *CyberChef Tool* to understand the basic features that you will use in the lab. https://vimeo.com/588599799

Part 1: Creating a Rainbow Table.

1. You are provided with a copy of the *Our Rainbow Table* file which is a spreadsheet that contains 5 passwords

2. Go to the CyberChef website at https://gchq.github.io/CyberChef/

3. On the left toolbar under OPERATIONS, type MD5 in the Search area. Drag the MD5 title over to the RECIPES section.

4. Type the first password into the INPUT section. CyberChef will automatically apply the MD5 Has algorithm to that plaintext and deliver the hash to the OUTPUT section.

5. Copy the hashed password into the MD5 Hashes column in the table.

6. Repeat steps 4 & 5 for the other four passwords

Part 2: Cracking Passwords with the Rainbow Table.

1. Select one of the hashes in the table and exchange with a partner.

2. Look up that hash in the table and confirm with your partner that you have identified the plaintext of their hash. They will do the same with the hash you provided. *This proves that you know each other's passwords from looking up the hash in your rainbow table.*

Part 3: Adding Salts for Security

1. Select a different password and type it into the INPUT section BUT add a unique string of 6 numbers (Ex: 583967). That number string is the salt for your password so keep it a secret. CyberChef will automatcially create a hash based on the password + the salt numbers.

2. Exchange salted hashes with a partner.

3. Look up the hashes in your rainbow table and confirm with your partner that neither hash can be found. *This proves that a salt protects hashed passwords from rainbow table attacks.*