Atelier2

Objectifs

L'objectif de cet atelier est de développer un script Shell ***password.sh*** permettant de tester et valider la robustesse des mots de passe. Le but est d'identifier les mots de passe faibles ou facilement devinables afin d'améliorer la sécurité.

Le script devra recevoir un mot de passe en entrée via un paramètre de la ligne de commande et vérifier sa conformité à des critères de sécurité prédéfinis.

Fonctionnalités

Un mot de passe est considéré comme **valide** s'il respecte les exigences suivantes :

- **Longueur minimale** : 8 caractères
- **Présence d'au moins un chiffre** (0-9)
- **Présence d'au moins un caractère spécial** parmi : @, #, $, %, &, *, +, -, =
- **Contrôle dictionnaire** : Toute séquence de **quatre caractères consécutifs ou plus** présente dans un dictionnaire standard doit entraîner un rejet du mot de passe.

Le script devra implémenter les fonctionnalités suivantes :

1. **Afficher l'usage** : Une fonction show_usage qui affiche un message d'aide sur la sortie standard avec la syntaxe d'utilisation :

   password.sh: [-h] [-v] [-t] mot de passe

2. **Vérifier la présence d'un argument** : Si aucun argument n'est fourni, afficher un message d'erreur et l'usage du script sur la sortie d'erreur.
3. **Tester la validité du mot de passe**.
4. **Afficher une aide détaillée** : Une fonction HELP permettant d'afficher un guide détaillé depuis un fichier texte.

Options

Le script devra proposer les options suivantes :

- `-t` : Vérification du mot de passe fourni en entrée.
- `-h` : Affichage de l'aide détaillée en lisant un fichier texte dédié.
- `-v` : Affichage du nom des auteurs et de la version du script.

Consignes

- Chaque option sélectionnée doit déclencher une fonction.
- L'utilisation de **getopts** est obligatoire pour gérer les options du script