Fonctionnalité gestionnaire de de m

**SAÉ 11 :**

*5 parties :*

-Bonnes pratiques : Complexité des MDP, force,

renouvellement, moyen mnémotechnique etc.

**. Complexité des MDP/Force :**

**Longueur** : Utiliser un grand nombre de caractères ; Plus un mot de passe est long, plus il est difficile à craquer.

**Complexité** : Combiner lettres majuscules/minuscules chiffres et caractères spéciaux (comme !, @, #, $, etc.).

**Pas de mots communs** : Éviter les mots du dictionnaire, les noms, et les séquences de touches (comme "123456" ou "qwerty").

**Unique** : Ne pas utiliser le même mot de passe pour plusieurs comptes. Si un compte est compromis, les autres le seront aussi.

**Gestion des mots de passe** : Utiliser un gestionnaire de mots de passe pour stocker et générer des mots de passe forts.( -> partie 5)

**Authentification à deux facteurs** : Activer cette option autant que possible pour ajouter une couche de sécurité supplémentaire.

**. Renouvellement :**

**Renouvellement régulier** : Changer mots de passe tous les 3 à 6 mois, surtout pour les comptes sensibles.

**Après une compromission** : Si suspicion qu'un compte a été compromis, changez immédiatement le mot de passe.

**Ne pas réutiliser les anciens mots de passe** : S’assurer que votre nouveau mot de passe n'a pas été utilisé précédemment.

**Suivi des changements** : Garder un enregistrement des dates de changement de mot de passe pour vous rappeler quand il est temps de les mettre à jour.

**Automatisation** : Autant que possible, utiliser un gestionnaire de mots de passe qui propose des rappels pour changer régulièrement les mots de passe.

**. Moyens mnémotechniques :**

**Passphrases** : Créer une phrase facile à retenir en utilisant une série de mots, par exemple : "MonChienJoueDansLeParc!". Cela peut être plus facile à mémoriser qu'un mot de passe complexe.

**Acronymes** : Prendre une phrase significative pour vous et créer un acronyme à partir des premières lettres. Par exemple, "Je vais à Paris en 2024!" pourrait devenir "JvPé2024!".

**Personnalisation** : Associer un mot de passe à un événement, un lieu ou une personne importante pour vous, en intégrant des éléments de sécurité.

**Moyens phonétiques** : se rappeler d’une expression souvent utilisée et la réinterpréter à l’aide de caractères spéciaux tout en gardant une ressemblance phonétique.

Sources : [https://secnumacademie.gouv.fr](https://secnumacademie.gouv.fr/content)

-**Force brute et dictionnaire**

Faire une wordlist de la cible et ensuite faire de la force brute

Liens/Sources :

**# Lot A : Mots de passe utilisateurs**

**# Bonnes pratiques**

**## Complexité des MDP**

**### Qu'est ce qu'un bon mot de passe ?**

Définition : On parle de mot de passe fort, lorsqu’un mot de passe apporte un niveau de sécurité suffisant. Lorsqu'il est difficile à découvrir par un attaquant dans un temps raisonnable, à l'aide d'outils automatisés de recherche qui mettent en œuvre les différentes techniques d'attaque vues précédemment.

**### Les règles d’or pour créer un bon mot de passe**

**#### A faire**

1) Utiliser le plus possible de caractères, au moins 10 caractères (Pour 10 caractères numériques, il existe 10 milliards de possibilités.)

2) Varier les caractères utilisés (plus vous utiliserez un éventail large de caractères, mieux votre mot de passe sera protégé,

3) Avoir des mots de passe uniques par application (Active Directory, messagerie, etc.) et par usage (professionnel, personnel)

4) Bannir tout mot issu d'un dictionnaire, ceux-ci sont testés dès le premier niveau d’attaque.

**#### A éviter**

1) Éviter les rapports psycho-sociaux évidents vous concernant (nom, prénom, date de naissance, prénom de vos parents/enfant(s), nom de votre animal de compagnie, etc.)

2) Éviter également les liens avec le nom du service pour lequel il est utilisé (ex : CréditAgricole5, mdpHotmail, etc.) ou encore avec sa fonction (ex : MaSociete25000, Adminserveurimprimerie, MDPmessagerie, etc.) ;

3) Eviter de remplacer des caractères de mots du dictionnaire par des caractères spéciaux (ex: mot2pA$$e!) => très simple à ,trouver

4) Éviter d’ajouter des signes de ponctuation en fin de mot.

5) Eviter les caractères accentués « é, è, à », etc. Ils ne sont pas toujours disponibles sur les claviers d’autres pays.

6) Ne pas prendre de mot de passe déjà existant, pris en exemple sur Internet.

**### Renouvellement**

Il n’est pas recommandé de forcer les utilisateurs à changer de mot de passe trop fréquemment !

Votre service informatique peut vous imposer de changer régulièrement votre mot de passe. Idéalement vous devriez choisir un nouveau mot de passe à chaque fois.

La plupart des gens qui changent leurs mots de passe ajoute seulement un caractère en plus ou un nombre (comme un compteur) à leur ancien mot de passe.(ex: feEgIsR#c1, feEgIsR#c2, feEgIsR#c3, etc.).

Il est donc simple pour une personne malveillant en possession de votre ancien mot de passe, de découvrir le nouveau,

**### Moyens mémotechniques**

Ne pas écrire ses mots de passe!

**#### Il existe plusieurs méthodes pour se souvenir de son mot de passe :**

1) Définir une phrase de passe (prendre plusieurs mots au hasard Lunettes:Crayon:Poste:Chemin », ou une vraie phrase "Vive la SAE11" ). Ces mots sont facilement mémorisables et difficilement trouvables.

2) Utiliser la phonétique, c’est-à-dire retenir les sons de chaque syllabe pour fabriquer une phrase facile à retenir.

(ex: « J'ai acheté huit CD pour cent euros cet après-midi » devient ght8CD%€7am, "Deux cadeaux à noël" devient 2KDO@nowel.)

Même si le système phonétique se rapproche beaucoup du langage SMS qu‘il est déconseillé d'utiliser, il peut cependant être acceptable dans le cas où l'on utilise une phrase de passe suffisamment longue et non un seul mot modifié.

3) Retenir les premières lettres d'une phrase comme une citation, ou encore les paroles d’une chanson.

Pour cette méthode, il faut cependant éviter les phrases trop communes, choisir une phrase suffisamment longue, et ne pas se limiter aux minuscules.

(ex: la citation « un tiens vaut mieux que deux tu l'auras » devient « 1Tvmq2tl@ »).

**#### Autres exemples :**

« Le bac et ensuite la fac » peut devenir « 1BAC,+1fac ».

« L'indicatif 33 pour la France » peut devenir « (+33)=Fra! ».

« Une opération de multiplication » peut devenir « op:12\*5=60 ».

**### Synthèse**

Enfin, il est possible de combiner plusieurs de ces méthodes, comme par exemple :

« Pie-Car:5\*5=25 ».

Retenez que ces différents moyens mnémotechniques vous permettront de définir des mots de passe sécurisés et faciles à retenir.

**# Gestion des mots de passe :**

**## Les principales fonctionnalités offerte par un gestionnaire de mot de passe**

**### A faire**

**#### Stockage sécurisé des mots de passe**

Les gestionnaires de mots de passe chiffrent les informations enregistrées, comme les mots de passe et les identifiants, afin qu’elles soient accessibles uniquement avec un mot de passe principal (ou "master password"). Seul cet unique mot de passe doit être mémorisé par l'utilisateur.

**#### Générateur de mots de passe forts**

La plupart des gestionnaires proposent un générateur de mots de passe aléatoires et robustes, permettant de créer des mots de passe complexes et difficiles à deviner. Ces mots de passe peuvent inclure des caractères spéciaux, des chiffres, des majuscules et minuscules, et être de longueur variable.

**#### Remplissage automatique**

Les gestionnaires peuvent automatiquement remplir les champs d'identification sur les sites web et applications, ce qui permet de gagner du temps et d'éviter les erreurs de saisie manuelle. Cette fonctionnalité est souvent disponible via des extensions de navigateur.

**#### Authentification multi-facteurs (2FA)**

En plus du mot de passe principal, certains gestionnaires intègrent une option d'authentification à deux facteurs (2FA) pour ajouter une couche supplémentaire de sécurité. Cela peut inclure des codes de validation envoyés par SMS, générés par une application d'authentification, ou des dispositifs matériels comme des clés de sécurité (YubiKey).

**#### Audits de sécurité**

Les gestionnaires de mots de passe peuvent analyser vos mots de passe enregistrés et vous informer des mots de passe faibles, réutilisés ou compromis dans des fuites de données. Ils peuvent également vous inciter à mettre à jour régulièrement vos mots de passe.

Sauvegarde des informations supplémentaires

En plus des mots de passe, les gestionnaires peuvent stocker d'autres types d'informations confidentielles comme des cartes bancaires, des notes sécurisées, des documents sensibles, etc.

(Se poser la question, Faut enlever ou pas??????)

**#### Accès d’urgence**

Certains gestionnaires offrent une fonctionnalité permettant de désigner un contact d’urgence qui peut accéder à vos mots de passe en cas de décès ou d'incapacité. Cette option est activée après une certaine période définie par l’utilisateur.

**### A éviter**

**#### Synchronisation multi-appareils**

Pour une gestion plus fluide, beaucoup de gestionnaires offrent la possibilité de synchroniser les mots de passe entre plusieurs appareils (ordinateur, smartphone, tablette). Les données sont généralement chiffrées avant d'être envoyées aux serveurs, garantissant ainsi une sécurité supplémentaire.

**#### Partage sécurisé de mots de passe**

Certains outils permettent de partager des mots de passe ou des informations sensibles avec d'autres utilisateurs de manière sécurisée. Cela peut être utile dans un contexte professionnel ou familial.

**#### Exportation et importation des mots de passe**

Pour faciliter la transition d’un gestionnaire de mots de passe à un autre, il est souvent possible d’importer ou d’exporter des mots de passe sous forme de fichiers chiffrés ou de formats spécifiques.

**## Les logiciels disponibles sur une distribution Debian pour gérer ses mots de passe.**

**### KeePassXC – Le plus sécurisé pour Debian**

**#### Pourquoi KeePassXC est le plus sécurisé :**

**#### Chiffrement robuste**

KeePassXC utilise un chiffrement AES-256 pour sécuriser les bases de données de mots de passe. Il s'agit d'une norme de chiffrement très puissante et largement reconnue comme étant pratiquement impossible à casser avec les technologies actuelles.

**#### Stockage local**

Contrairement à d'autres solutions qui stockent les données dans le cloud, KeePassXC stocke les mots de passe localement sur votre appareil. Cela réduit considérablement le risque lié aux violations de données sur des serveurs distants.

**#### Fichiers clés et doubles facteurs**

En plus d’un mot de passe principal, KeePassXC permet d’utiliser un fichier clé (key file) pour déverrouiller la base de données, ajoutant ainsi une couche de sécurité supplémentaire. Vous pouvez aussi l’intégrer avec des solutions d’authentification à deux facteurs (2FA).

**#### Open-source**

KeePassXC est entièrement open-source, ce qui signifie que son code est examiné par des experts en sécurité du monde entier. Cela garantit qu'il n'y a pas de failles cachées ou de portes dérobées (backdoors).

**#### Résistance aux attaques**

KeePassXC utilise des techniques comme PBKDF2 et Argon2 (algorithmes de dérivation de clés) pour protéger les mots de passe, les rendant résistants aux attaques par force brute.

**#### Hors-ligne**

KeePassXC fonctionne hors ligne, ce qui signifie qu’il n’est pas exposé aux attaques réseau lorsqu'il n'est pas utilisé pour synchroniser des données avec des services externes.

**#### Multiplateforme et intégrations**

En plus de Debian, KeePassXC est disponible sur d'autres systèmes d'exploitation et peut s’intégrer avec des extensions de navigateur pour un remplissage automatique des mots de passe de manière sécurisée.

**### Installation de KeePassXC sur Debian :**

Pour installer KeePassXC sur Debian, il suffit de lancer la commande suivante :

Commande : sudo apt install keepassxc

Source : https://keepassxc.org/