Tp 2

1. Aperçu
2. Objectif du lab
3. Consignes
   3.1. Découverte de l'outil

Lorsqu'il s'agit de stocker des informations confidentielles, il convient de s'assurer que celles-ci sont enregistrées de manière sûr. En parcourant le site officiel de Keepass, trouvez, pour la version du logiciel que vous utilisez, sous quelle forme sont stockés les mots de passe enregistrés dans le logiciel, et quel(s) algorithme(s) est(sont) utilisé(s) pour cela ?

Le logiciel open source KeePass est un « coffre-fort » de mots de passe qu'il stocke dans une base de données dont l'accès est authentifié et le contenu chiffré.
Les codes sont chiffrés en HMAC-SHA-256 dans un fichier unique. (AES/Rijndael ou ChaCha20)

En consultant le site de l'ANSSI2, expliquez ensuite pourquoi il plus prudent d'utiliser la version 2.41 de Keepass plutôt que la version 1.36.

https://keepass.info/compare.html

Téléchargez la dernière version portable stable de Keepass sur votre poste.

Keypass 2.41

3.2. Configuration et utilisation du gestionnaire de mot de passe
   3.2.1.Etapes préliminaires

Créez un compte utilisateur sur votre poste. Celui-ci devra disposer d'un mot de passe fort, et être membre du groupe « Administrateurs ».
Ouvrez Keepass, puis renseignez un « Master Password » d'au moins 15 caractères variés, à l'aide d'une des deux méthodes4 indiquées en cours.

Je sais que tu t'appelle billy et que tu vis à NewYork
JCK3tutAplB1l1EK3tu@aGA (23 caractères)

   3.2.2.Utilisation de l'outil

Dans Keepass, enregistrez les deux comptes suivants ;
Le compte Administrateur que vous venez de créer, dans la section « Windows ». Ce compte vous servira à démarrer une application avec une élévation de privilège, cmd.exe par exemple. votre compte YNOV dans la section « email ».
Connectez-vous ensuite, à l'aide de ces deux comptes, des deux façons suivantes :
d'abord en copiant le mot de passe dans le clipboard, via l'option dans Keepass, puis en utilisant la fonctionnalité auto-type.

3.3. Fonctionnalités annexes du gestionnaire de mot de passe
   3.3.1.Générateur de mot de passe

Keepass vous permet également de générer des mots de passe. Vous modifierez donc le « Master Password » de votre database, en utilisant le générateur de mots de passe de Keepass. Vous respecterez les contraintes de complexité imposées précédemment pour la génération de ce mot de passe.

4#OmB!1Gl;/rZ^XK,r1?

3.3.2. Taches automatisées

Keepass permet de mettre en oeuvre des tâches automatisées.

• Expliquez la fonctionnalité « Triggers » intégrée à Keepass.

• Vous créerez alors un Trigger qui permettra de sauvegarder la base automatiquement à la fermeture de Keepass. Ce Trigger ne devra conserver que 3 exemplaires de la base de données dans son historique.

Triggers : Action programmée réagissant à un évènement (exemple : sauvegarde de la BDD quand on ferme keepass

3.4. Sécurisation de la solution

Une fois la solution mise en oeuvre, il convient de sécuriser son utilisation. Vous mettrez donc en oeuvre les deux mesures de sécurité suivantes :

• vous « imprimerez » la feuille « d'urgence », qui permettra de conserver le « Master Password » en lieu sûr.

• Vous créerez ensuite un script avec Robocopy5 qui permettra de sauvegarder la base de données.